Cluster Computing (2024) 27:14637–14668
https://doi.org/10.1007/s10586-024-04662-6

DDoS attack detection techniques in IoT networks: a survey

Amir Pakmehr[1,2] · Andreas Aßmuth[1] · Negar Taheri[3] · Ali Ghaffari[3,4,5]

Received: 8 February 2024 / Revised: 13 June 2024 / Accepted: 5 July 2024 / Published online: 26 July 2024

Abstract
The Internet of Things (IoT) is a rapidly emerging technology that has become more valuable and vital in our daily lives. This technology enables connection and communication between objects and devices and allows these objects to exchange information and perform intelligent operations with each other. However, due to the scale of the network, the heterogeneity of the network, the insecurity of many of these devices, and privacy protection, it faces several challenges. In the last decade, distributed DDoS attacks in IoT networks have become one of the growing challenges that require serious attention and investigation. DDoS attacks take advantage of the limited resources available on IoT devices, which disrupts the functionality of IoT-connected applications and services. This article comprehensively examines the effects of DDoS attacks in the context of the IoT, which cause significant harm to existing systems. Also, this paper investigates several solutions to identify and deal with this type of attack. Finally, this study suggests a broad line of research in the field of IoT security, dedicated to examining how to adapt to current challenges and predicting future trends.

Keywords Internet of Things · DDoS · Intrusion detection · Machine learning

Abbreviations

DNS	Domain name system
DBN	Deep belief networks
DDoS	Distributed denial of services
IoT	Internet of Things
CNN	Convolutional neural network
SDN	Software defined networking
DoS	Denial of services
IDS	Intrusion detection system
SOM	Self−organization map
TAMD	Traffic analysis and malware detection
RBM	Restricted Boltzmann machines
CFS	Correlation based feature selection
RFID	Radio frequency identification
LRDDoS	Low−rate distributed denial of service
OSI	Open systems interconnection
BC	Block chain
UDP	User datagram protocol

✉ Ali Ghaffari
a.ghafari@iaut.ac.ir

Amir Pakmehr
a.pakmehr@oth-aw.de

Andreas Aßmuth
a.assmuth@oth-aw.de

Negar Taheri
negartaheri@iaut.ac.ir

[1] Department of Electrical Engineering, Media and Computer Science, Ostbayerische Technische Hochschule Amberg-Weiden, Amberg, Germany

[2] Department of Computer and Information Technology Engineering, Qazvin Branch, Islamic Azad University, Qazvin, Iran

[3] Department of Computer Engineering, Tabriz Branch, Islamic Azad University, Tabriz, Iran

[4] Department of Computer Engineering, Faculty of Engineering and Natural Science, Istinye University, Istanbul, Turkey

[5] Department of Computer Engineering, Khazar University, Baku, Azerbaijan

1 Introduction

The Internet of Things is an intelligent network that connects billions of various devices to the Internet using the IP (e.g., IPv4 or IPv6) protocol. This network provides unique addressing capabilities to devices and objects, enabling them not only to identify themselves but also to directly communicate with each other and collect data generated by other IoT devices. Furthermore, these devices are capable of transmitting data without the need for human

intervention [1–3]. IoT due to wider connection, more data [4], limited resources of devices, such as data storage and processing units, flexibility and that it can be used in various fields such as smart homes, smart cities, industry, smart healthcare, smart agriculture, etc. The versatility of these applications enables the IoT to serve as an alternative to traditional networks in various contexts [5–7]. This network is defined in a way that allows anyone to have direct access to anything, anytime, and from anywhere, and it is recognized as a dynamic global infrastructure. The use of IoT devices in various fields such as supply chain management, healthcare, industry, physical security, agriculture, and even home automation has led to transformation and improvement in these areas [8–10].

Figure 1 shows the layered structure of the IoT, which includes three layers and three different functions. The first layer, also known as the perception layer, is responsible for collecting data from sensors and various devices in the IoT. The perception layer uses wired and close-range wireless communication technologies [11, 12] like RFID, NFC, etc. to establish communication between devices and sensors. This layer transfers environmental information to the network layer to be used in the process of communication and data management in the IoT network. It is also referred to as the sensor layer. The collected information is then converted into digital signals in preparation for transmission to the network layer. The second layer is the network layer, which is responsible for managing communication between devices and objects. It acts as the brain of the IoT and is a center for the Internet network, intelligent processing, and network management center. This layer employs diverse communication protocols such as Bluetooth, Wi-Fi, ZigBee, and others to send and receive data. The network layer acts as an intermediary between the Perception layer and the application layer in the structure of the IoT. It received from objects in the perception layer, transmitted, and processed in this layer. This layer connects various smart objects, servers, and other devices in the network. These applications make intelligent decisions using the data collected by sensors and network communications and improve and optimize the process. The application layer in the architecture of the IoT acts as the highest layer, responsible for providing specific services, bridging social and industrial aspects, validation, confidentiality, authenticity and reliability of data. It plays a fundamental role in shaping the user experience and facilitating the integration of artificial intelligence into IoT applications (Fig. 2).

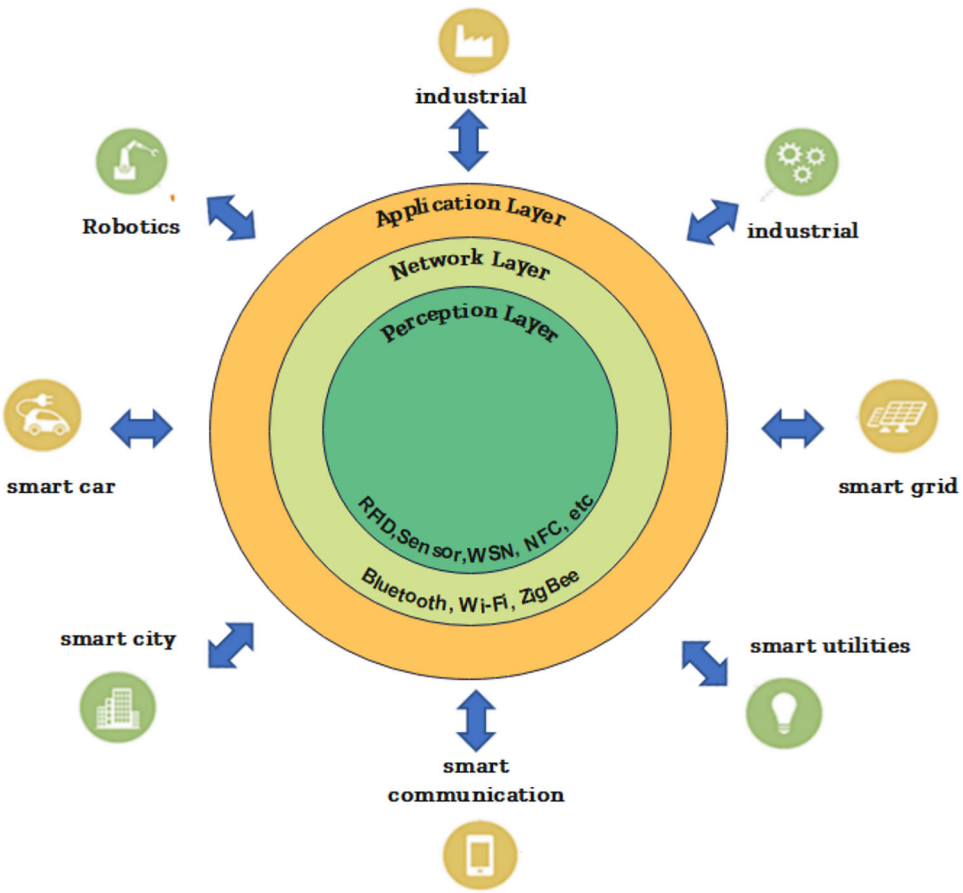

Fig. 1 IoT structure

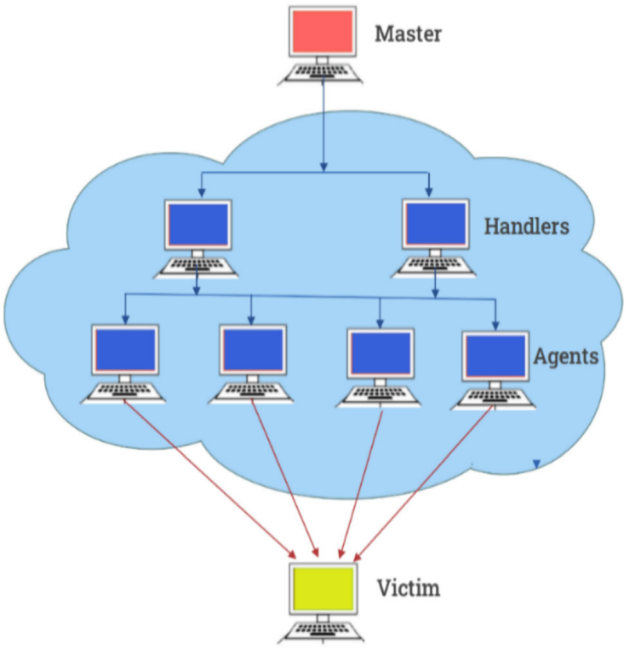

Fig. 2 Components constituting DDoS attacks

Some challenges hinder the realization of the IoT, such as scalability [13], openness, reliability, architecture and its dependencies, large data volumes, security, and privacy [14–16]. Moreover, the issue of vulnerabilities in IoT systems can be attributed to the physical constraints of IoT devices, which encompass limitations in terms of computational capabilities, internal storage capacity, and battery life [17, 18]. Additionally, the absence of consensus or standardization in security protocols for IoT, along with the prevalent use of third-party hardware, software, and firmware, further exacerbates this problem. When alternate solutions are not feasible, these systems frequently lack sufficient security measures. The constrained resources found in typical IoT devices render the utilization of intricate and time-consuming encryption/decryption algorithms for secure message communication impractical [19–21]. This makes IoT systems highly susceptible to various types of attacks. With the increasing number of Internet-connected devices, the number of attack points and the available capabilities for hackers to conduct attacks are on the rise. On the other hand, a system's vulnerability to security attacks and its resistance against these attacks is caused by bad configuration and causes vulnerability [14, 22, 23].

Therefore, security in IoT devices and networks is of paramount importance.

To address the security challenges associated with IoT, it is essential to implement appropriate security standards and solutions. This includes the use of strong encryption to protect data transmission, robust authentication and access control, regular and secure updates for devices' operating systems and firmware, in addition, security by design should be one of the main concerns of the manufacturer.

1.1 Privacy and security challenges on the Internet of Things

Considering the growth and evolution of the IoT domain and the increasing number and variety of devices that integrate connectivity capabilities, security features must also expand proportionally. IoT devices are often produced under high price pressure. That's the reason why many manufacturers don't implement the necessary security measures because that would make the devices more expensive [24, 25]. By developing security capabilities, we can achieve greater security and privacy in the IoT domain [26–28]. This section provides an overview of the security challenges emphasized in the IoT environment, along with an examination of potential solutions.

1.1.1 Confidentiality

Information security is considered as a fundamental factor in maintaining data confidentiality. Some IoT devices need to manage information and must be categorized in a way that preserves their confidentiality. Confidentiality stands as a paramount concern in network security. In its essence, it ensures that each node maintains the confidentiality of its data, prohibiting sharing with neighboring nodes. Additionally, it possesses the capability to conceal messages from passive attackers, ensuring that any information transmitted through the sensor network remains confidential. This can encompass a wide range of sensitive data, such as smart meter measurements, billing details, personal information, demographic data, and more.

1.1.2 Integrity

Ensuring the accuracy of data exchange between multiple IoT devices is of great importance. This requires ensuring that the data originates from the correct source and remains unchanged during its transmission. To illustrate this point, let's consider the scenario of storing medical patient information. It is essential that this data remains unchanged. To provide effective protection for the integrity service, it is beneficial to use message integrity codes and hash function mechanisms. In addition, maintaining end-to-end security communications in the IoT is very important to maintain the integrity feature. This requires establishing secure communication channels from the source device to the destination device, thereby maintaining the integrity of the transmitted data. By implementing these

measures, the integrity of data exchange in IoT ecosystems can be effectively maintained.

1.1.3 Availability

The primary foundation of the IoT is the establishment of connections between a vast array of devices and objects. The notion of availability holds significant importance within this framework, as it aims to guarantee that all data pertaining to these objects remains readily accessible whenever the need arises. Within the realm of the IoT, the utilization of the data component always necessitates both the availability and accessibility of devices and services.

Privacy and security concerns are prevalent in the realm of IoT technologies, giving rise to a multitude of challenges. The primary objective behind the malevolent actions of attackers is to exploit vulnerabilities inherent in operating systems and IoT technologies, leading to detrimental consequences such as data breaches and theft.

The spectrum of malicious cyber-Attacks is wide-ranging and encompasses various tactics. Unauthorized access, social engineering, the deployment of malware, destructive cyber intrusion endeavors, and even physical theft are among the diverse strategies utilized by nefarious [29, 30]. In essence, these threats collectively pose significant risks to the integrity and confidentiality of IoT systems, necessitating robust measures to safeguard against potential breaches, including:

1.1.4 Cyber-attack

A cyber-Attack in IoT means disrupting the functioning of networks/systems using hacking tools and methods, to exploit the systems to retrieve valuable information or for personal satisfaction. Kinds of Cyber Assaults range from obtaining authentication information to targeting unencrypted traffic in pursuit of Valuable Data. Cybercriminals can be from government institutions to private companies, and behind cyber-Attacks, they are considered a substantial threat to the new smart world.

1.1.5 Challenges in software and hardware systems

Discerning challenges and vulnerabilities are achievable in software [31–33] and hardware systems in many parts of the operating system or IoT networks. These challenges include weaknesses in software systems, networks, procedures, and policies. Two main components have been identified in IoT: software and hardware systems. Vulnerabilities can be identified at the software system level, among application software, operating systems, and controls. Also, lack of proper planning, insufficient communication, insufficient knowledge, and lack of resources in hardware and software systems are among the factors that can lead to vulnerabilities in IoT systems and affect the security and privacy of users.

1.1.6 Unauthorized access and reconnaissance

Unauthorized access attacks in IoT systems and devices can be categorized into two different types: remote access attacks and physical access attacks. The former involves accessing systems and devices via the Internet and IP-connected devices, while the latter involves criminals physically targeting the technologies themselves. These attacks pose a significant threat to outdoor and unattended IoT technologies. One attack, known as a reconnaissance attack, is often underestimated by security officers in denial-of-service attacks or backdoor access attacks. This attack involves collecting sensitive information from the operating system. Strategies utilized in these attacks encompass activities like mapping the network, identifying vulnerabilities and technology services through packet sniffers, soliciting IP address information, and probing system ports.

1.1.7 Lexical assaults and robust crackdowns

IoT faces serious privacy threats, particularly concerning passwords. Bad actors, whether individuals or groups, use dictionary and brute force attacks to replicate valid user passwords. In a dictionary attack, hackers try various combinations of letters and numbers, while brute force attacks systematically crack numerous password combinations to find the correct one.

1.2 The challenges of DDoS attacks on IoT

There are also two aspects to DDoS attacks and IoT devices:

(a) a DDoS attack against a specific IoT device, for example, to prevent it from functioning properly, for example, to prevent sensor data from being sent to a server or cloud service [34].
(b) IoT devices that have been captured and controlled by an adversary and that adversary uses these devices to launch a DDoS attack against any other service on the Internet.

In this type of attack, attackers use multiple different devices to send a high volume of traffic to the target This causes the server to become unavailable or reduces the response speed to authorized users [35, 36]. Hackers take advantage of the vulnerabilities in IoT devices [37], leveraging their weaknesses to deploy malicious software known as Trojans, which are then distributed through email

campaigns or advertisements. Once these Trojans infiltrate the compromised devices, they can transform them into obedient zombies, ready to carry out the hackers' commands. These compromised devices, now under the control of the hackers, play a crucial role in launching Distributed Denial of Service attacks on servers and target networks, causing significant disruptions and potential security breaches [38]. Studies show that DDoS attacks are more often targeted towards gaming applications and the telecommunications industry [39]. In terms of security issues, securing the IoT involves addressing complex challenges and vulnerabilities to counter various attacks. Identifying and mitigating system vulnerabilities are crucial steps in ensuring network security and preventing potential intrusions. In addition to the above, users must be vigilant about potential security risks in IoT devices, as their connection to the Internet can expose them to vulnerabilities. Security systems should offer control and monitoring features for users to oversee and manage device activities, enabling prompt action in case of anomalies. Table 1 provides a list of key vulnerabilities that allow attacks on IoT devices.

1.3 Components of DDoS attacks

The attacker using a master and several agents tries to attack a victim using vulnerable hosts (handler). Handlers can be programs installed on a set of affected devices, and attackers use them to send various commands to the agents and control them through the controller. Agents are devices that have been compromised by controllers and function as attack tools against the victim system. Hosts executing these attack tools are recognized as bots or zombies. Nevertheless, identifying and mitigating these attacks is quite challenging, and various techniques are being considered to identify and classify DDoS attacks.

In this paper, we investigate DDoS flood attacks and detection mechanisms in IoT network systems. Examining DDoS flood attacks and detection methods in IoT networks, this paper aims to classify these attacks and explore detection and defense mechanisms based on timing and location. The research provides insights into IoT security challenges, contributing to the development of more effective defense strategies against DDoS flood attacks. The main contributions of this paper are as follows:

- Investigating the DDoS attacks and detection mechanisms in IoT
- Classifying DDoS attacks in IoT and exploring the detection and defense mechanisms
- Providing issues and challenges in IoT security and further research directions

The rest of this article is structured as follows: Sect. 2 presents the research background on DDoS attack detection. Section 3 deals with the classification of DDoS attacks. Section 4 describes defense mechanisms and intrusion detection techniques in DDoS attacks, accompanied by a comparative table of their advantages and disadvantages. Section 5 describes several open research issues and challenges needed to achieve comprehensive protection against DDoS attacks. Section 6 deals with the general summary and conclusions.

2 Research background

In a DDoS attack, botnets are utilized, allowing attackers to use compromised computers to send an overwhelming volume of simultaneous requests to a target. The primary goal is to overwhelm the target's resources, such as bandwidth and server capacity, exceeding their capacity to handle the requests. Additionally, DDoS attacks may involve DNS amplification, exploiting vulnerable DNS

Table 1 Identification of current weaknesses and bad configuration on the Internet of Things

Bad configuration	Weak points
Weak IoT Authentication: Default or weak credentials may lead to unauthorized access and security breaches	lack of authentication, insecure protective credentials, non-use of encryption, storing passwords on the device
Insecure Network Settings: Misconfigurations in IoT network settings, can expose devices to external threats	Insecure network services on Internet-connected devices, including untrusted web services, insecure FTP, and DNS services, pose security risks and expose vulnerabilities in IoT devices
Lack of Encryption: Risks of Unprotected Data in IoT Transmission	Poor implementation and defects in security settings, weak login credentials, uploading files without user confirmation, uploading malicious codes
Unnecessary Services or Features on IoT devices can create additional attack surfaces, increasing the risk of exploitation	Lack of security support on devices, disabling of security features, lack of device updates, insufficient system monitoring
Poor Update and Patch Management may remain vulnerable to known exploits	Due to insufficient security configuration, lack of detailed permissions

servers to amplify the impact of the attack traffic. To detect DDoS attacks, various methods are employed.

- *Signature-Based Detection*: Recognizing known attack patterns by using predefined signatures.
- *Setting Thresholds*: Implementing rate limits to filter out excessive requests.
- *Connection Limits*: Restricting the number of connections from a single IP address.
- *User Behavior Analysis*: Examining patterns of user behavior to identify anomalies.
- *Machine Learning*: Using algorithms to detect unusual patterns in real-time.

In [40], three methods for DDoS attack detection in the IoT based on specific network behavior (feature extraction), SDN-based network architecture [41, 42], and a third approach from Apache Spark, which is a platform for DDoS attack detection in the IoT through machine learning were presented. Three introduced approaches used machine learning techniques to detect DDoS attacks in IoT. All three approaches provided comparable accuracy in detecting DDoS attacks. In [43], specific methods were employed to review concepts related to protection against DDoS attacks in the context of the IoT. Different defense techniques against DDoS attacks were analyzed and compared for the purpose of identifying vulnerabilities in them. They used approaches such as DDoS defense models based on IoT middleware, DDoS defense models based on machine learning detection and other defense mechanisms. Also, significant aspects and limitations of these methods are outlined, characterizing them as their vulnerabilities. In [44], published in 2020, they used an SDN-based framework as one of the effective strategies for detecting and mitigating DDoS attacks. This SDN-based approach also provided the capability to defend against DDoS attacks and allowed for centralized management of security and network analysis systems. This action enabled networks to rapidly respond with precise configurations and timely countermeasures to DDoS attacks. In [45], the authors investigated various defense methods against DDoS attacks. These methods include leveraging entropy changes [46] and other traffic anomalies as DDoS attack detection indicators, employing neural networks [47] was to identify and predict DDoS attacks, alongside using DDoS application layer defense methods to protect various services in networks. In addition to current defense are also explored. So far, research efforts to defend against DDoS attacks have not been validated in practice across a diverse range of networks.

In [48], the authors propose general methods for investigating DDoS attacks and their different types are introduced. In addition, diverse solutions for detecting and preventing DDoS attacks have also been explored. These solutions included tracking mechanisms, classified IP tracking, packet marking, entropy diversity, the use of network firewalls, CDN services, increased bandwidth, dedicated network equipment, and cloud-based security services. Each of these different techniques had its own advantages and disadvantages. In [49], the authors categorized defensive mechanisms against DDoS attacks. They classified these defensive mechanisms with the in pursuit of preventing DDoS attacks, detecting DDoS attacks, responding with DDoS attacks, and mitigating and tolerating with DDoS attacks. Despite the extensive efforts invested in developing techniques and defensive mechanisms against DDoS attacks, there were many challenges in this field. In [50], the researchers conducted their survey on detection and defense strategies against DDoS attacks in applications, web services, cloud computing, and internet-connected devices. They utilized intelligent computational techniques for the detection and prevention of DDoS attacks. They introduced a Multilayer Perceptron model for classifying attacks in a dataset and obtained very high accuracy [51]. Through a comprehensive analysis of these techniques, they examined the challenges related to DDoS attack identification and prevention.

In [52], a systematic analysis of DDoS attacks in non-traditional networks was presented. It includes categorization of different types of DDoS attacks and prevention techniques using filters, such as ingress/egress filters, filtering Martian addresses, and source address validation. Packet filtering based on the path and other mechanisms, attack detection methods, were also discussed. In [53], the authors presented various techniques to counter DDoS attacks. These techniques fall into three main categories: attack defense (load balancing and throttling), attack detection (probable packet marking), and attack filtering. Every one of these groups presented different methods and techniques to deal with DDoS attacks. This segmentation and description can help protect against DDoS attacks. In [54], different methods for detecting and preventing DDoS attacks at different levels are presented. They used various approaches, including monitoring the number of TTL tags of packets, entropy-based anomaly detection, packet filtering methods, intrusion detection system using Dumpster Shafter theory [55] to detect and prevent DDoS attack in cloud computing systems and performing a comparative analysis between them. Each of these defense techniques against DDoS attacks has its advantages and disadvantages. Some of the defense techniques are deployed in centralized network nodes, some in virtual machines, and others in cloud databases.

In [56], network anomaly detection using artificial intelligence and machine learning was reviewed and analyzed. By distinguishing normal and abnormal behaviors and analyzing network traffic to discover new attacks, it

has introduced various methods and models to increase network security. Also, it has evaluated the performance of Different techniques using actual data from network traffic and presented the results for intrusion detection in different systems. By utilizing artificial intelligence and machine learning technologies, this paper increases the ability to detect large and new attacks and enables the detection of "zero-day" attacks.

Table 2 presents a summary of the findings of several previously mentioned research studies, particularly in the field of detecting DDoS attacks. These findings include various aspects such as the techniques used, the goals pursued, the advantages and disadvantages encountered, and the results of using the selected data set to implement the proposed method.

2.1 Dealing with DDoS attacks on the Internet of Things

Addressing DDoS attacks in the context of the IoT requires a multifaceted approach that includes prevention, detection, and response strategies. Regarding how to deal with DDoS attacks, a multifaceted approach that includes prevention, detection, and response strategies is required. Key measures include network segmentation, traffic filtering, anomaly detection, device authentication, regular updates, traffic cleaning services, incident response planning, collaboration with ISPs, hybrid cloud solutions, and vigilant monitoring with reporting capabilities for early anomaly detection and rapid response [57].

3 Classification of DDoS attacks in IoT

DDoS attacks in the context of the IoT can take various forms. Here are some common types of DDoS attacks that specifically target IoT devices and systems. This categorization is illustrated in Fig. 3.

3.1 Application and transport layer attacks

Application Layer Attacks and Transport Layer Attacks refer to specific types of cyber-attacks that target vulnerabilities and weaknesses in the respective layers of the OSI model [58].

3.1.1 UDP flood attack

An HTTP Flood attack is a variation of DDoS attack in which the attacker illegitimately consumes system resources by sending an overwhelming amount of HTTP requests to the server, resulting in reduced speed and service unavailability. To execute this attack, the attacker typically utilizes their computer programs or zombie networks (Botnets) to send numerous HTTP requests to the target server. These requests can include GET, POST, or HEAD requests and are usually sent using an array of different IP addresses. Using HTTP requests, the attacker tries to tailor her traffic to make it less distinguishable and separated from typical web traffic (Tables 3, 4, 5, 6,7).

3.1.2 ICMP flood attack

"ICMP Flood attack" or "Smurf Attack" is a form of attack where the attacker sends high traffic towards a victim computer using ICMP Echo messages through one or more weaker broadcast stations. In this attack, the attacker employs a spoofed source address in ICMP echo messages to direct responses to the broadcast station. Subsequently, the broadcasting station amplifies the number of echo messages by responding to them, sending even more traffic towards the victim's computer. This significant traffic load can slow down the victim's computer and may even result in its downtime. The primary goal of an ICMP flood attack is to overwhelm the target device or network with many ICMP packets. IoT devices might struggle to handle the high volume of incoming requests, leading to increased processing overhead. The cumulative effect can result in a denial of service, rendering IoT services and communication channels inaccessible.

3.1.3 DNS attack

Domain Name System Amplification attacks are a type of network attack that involves using DNS servers to send extensive responses to small queries, with the aim of causing disruption and increasing network traffic volume. In these attacks, the attacker sends DNS queries to DNS servers using a forged IP address and requests them to send extensive responses to the target IP address. By sending small queries and receiving extensive responses, the network traffic volume increases disproportionately and can lead to network disruption and the loss of desired services. This type of attack utilizes DNS servers as a point of vulnerability and can cause significant disruptions in the network by employing reflection and traffic amplification techniques.

3.1.4 CLDAP attack

A CLDAP assault within the context of IoT pertains to the exploitation of CLDAP servers within IoT devices or networks for malicious intentions. CLDAP is a lightweight and connectionless protocol widely utilized in directory services. In a CLDAP assault, malevolent actors exploit vulnerabilities or misconfigurations in CLDAP servers to

Table 2 Comparison of some previous methods for detecting DDoS attacks in IoT

Diagnosis result	Disadvantage	Advantages	Target	Scheme	Refs
SVM, KNN, FR had high accuracy in classification	Weaknesses of linear SVM, time-consuming KNN, and real-time suitability issues with RF	Efficient Computing with ANN, resource-Efficient machine learning, and reducing false positives with SDN	Provide effective methods for countering DDoS attacks	Machine learning	[46]
Higher accuracy in defense mechanisms with training challenges	Resource demand, complexity, network overweight, and high costs in memory and time monitoring“	Enhancing efficiency: minimizing positive errors, short-term conditions, and early attack detection	Analysis and improvement of defense techniques against DDoS attacks	Detection technique based ML, based-middleware	[47]
High-precision network traffic analysis through SDN	High bandwidth requirements Dependence on SDN settings	Ability to learn dynamically Identification of different types of pests Using different algorithms	Security in IoT, detection and prevention of attack traffic in the network	SDN Based Detection Technique	[48]
Need for testing, validation, and additional solutions to counter attacks	Computational complexity, limited testing environment, and parameter testing constraints	Enhancing server security against DDoS Attacks Data sharing and collaboration	Approaches for monitoring network to detect spatio-temporal traffic patterns during DDoS attacks	-Defense techniques based on Entropy-Based, Neural Networks, Tracking, and Filtering	
Capable of detecting malicious activities Effectiveness with minimal user impact and inherent challenges	Vulnerability to algorithm deception High memory consumption and poor Performance High false alert rate, -slow convergence rate	Using various techniques to help identify attacks	Analysis of methods for detecting and countering DDoS attacks and reducing their impact	-Path reconstruction methods.—Entropy change and intrusion detection and prevention systems	
The need for multiple solutions to choose suitable ones	Time-consuming and complex Anomaly-based techniques may result in higher false alarms due to the analysis of unusual patterns	Wide coverage	A comprehensive overview of DDoS attacks Strategies to deal with them	Using a research and review approach	
Using computational intelligence for diagnosis Absence of a complete defensive solution	Lack of robust solutions Challenges in data aggregation and real-time analysis Reduced resistance to new attacks	Utilizing computational intelligence Emphasis on the necessity of up-to-date datasets	Developing an optimal, comprehensive, and precise defense system	Utilize computational intelligence strategies	
Accuracy enhancement in detection through threshold updating	Inconsistent filtering, signature-based limitations, and anomaly detection threshold issues	Using filtering to reduce server processing load by removing unwanted traffic	Complete review of DDoS attacks Methods of preventing and reducing them	DDoS attack detection and prevention techniques	
Comprehensive techniques for DDoS attack mitigation	Management complexity, decreased speed, firewall limitations, and frequent IP address changes	Load balancing Probable packet marking DDoS protection systems	Comprehensive analysis of DDoS attacks and defense methods	Strategies for Mitigating Attacks: Prevention, Tracking, and Filtering	
Prioritized router coordination, enhanced filter management through load balancing, and efficient attack mitigation	The need to improve proactive filtering systems	Accelerated propagation barriers, improved response speed, and adaptability against diverse attacks	A complete overview of filter-based defenses against DDoS attacks	Filtering techniques	

Table 2 (continued)

Diagnosis result	Disadvantage	Advantages	Target	Scheme	Refs
Utilizing ML techniques leads to increased accuracy in network attack detection	Computational complexity. - Limitation in detecting new attacks	Ability to detect widespread and new attacks Utilization of real-time data Capability to detect zero-day attacks	Intrusion detection by distinguishing between normal and abnormal behaviors during network traffic analysis	Deep learning techniques for intrusion detection in IoT environment	

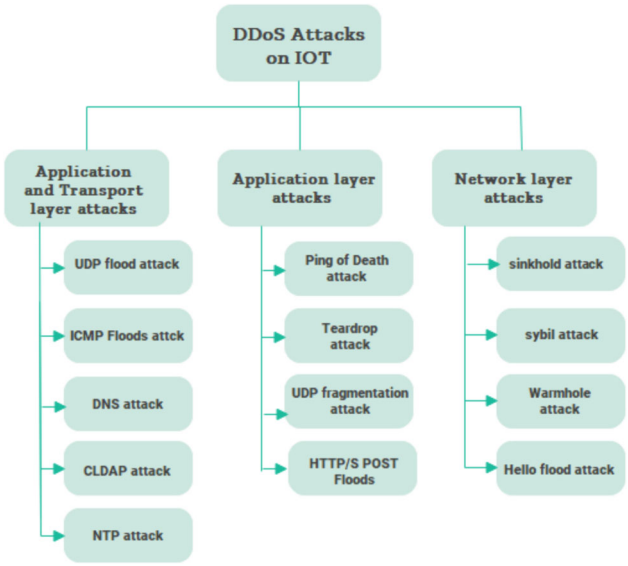

Fig. 3 Taxonomy of DDoS attacks across various IoT layers

initiate various forms of cyber assaults, encompassing reflection/amplification assaults for Distributed Denial of Service and other security risks. CLDAP assaults present a grave threat to IoT environments, and proactive actions are imperative to alleviate their repercussions. Consistent monitoring, the sharing of threat intelligence, and collaboration within the IoT community are indispensable for remaining ahead of emerging threats and safeguarding against CLDAP-associated vulnerabilities.

3.1.5 NTP attack

The Network Time Protocol (NTP) attack is one of the types of DDoS attacks. In this type of attack, the attacker sends many forged NTP requests to publicly unavailable NTP servers. These requests are designed in a way that they appear to originate from the target server or network, thus deceiving NTP servers into sending much larger responses than the original request to the target. This

Table 3 signature-based techniques

Diagnosis result	Real-time detection	Advantages and disadvantages	Algorithm/model	Technique
This approach enhances network security and has a 100% True detection rate with high precision	×	Advantages: Implementation of IDS, using open and expense-free sources Disadvantages: Lack of detection of new attacks Need for powerful hardware and software equipment Need for high costs due to the complexity of error generation	SNORT	Signature-based Intrusion Detection System (IDS) utilizing the open-source program SNORT [62]
It enhances the power and efficiency of signature-based intrusion detection systems in hostile environments	×	Disadvantages: Requirement for high computational power and cost in real-world scenarios Advantages: Increased detection power and efficiency Secure sharing and updating of signature database	Blockchain	Detection based on blockchain signatures CBSigIDS [63]

amplification effect allows the attacker to create a significant traffic volume with a relatively minor effort.

3.2 Application layer attacks

3.2.1 Ping of death

The "Ping of Death" attack involves sending ICMP echo requests larger in size than the maximum standard size of IP packets, resulting in server crashes. Larger packet sizes are then divided into smaller segments and transmitted as multiple packets. The attacker sends several packets that surpass the maximum bytes to the victim, which, when combined, significantly exceed the byte threshold. Surpassing the threshold leads to elevated cache memory usage, which in turn causes system instability. After the system has become compromised, It gowns more vulnerable to other attacks like the Trojan horse attack [59].

3.2.2 Teardrop attack

The Teardrop attack manipulates the offset values in fragmented packets at the application layer, exploiting vulnerabilities in the reassembly process. In networking, large packets are divided into fragments for transmission, and the receiving system reassembles them. By intentionally setting confusing offset values in the IP header, the attacker aims to disrupt reassembly. If the receiving system mishandles overlapping fragments, it can lead to errors or crashes. The Teardrop attack seeks to destabilize or crash the target system, causing a denial of service and hindering legitimate user access to the targeted application or service.

3.2.3 UDP fragmentation attack

A UDP fragmentation attack, also known as a form of UDP flooding, requires the transmission of significant packets to optimize the use of available bandwidth while minimizing the size of messages. In this form of attack, the malicious actor takes advantage of the lack of a real connection between the spoofed frames, thus forcing the target server to exhaust its CPU resources trying to "reassemble" these nonsense packets. Transparent CPU usage has the potential to cause overheating and subsequent system reboots. Identifying this attack is difficult due to its similarity to regular traffic.

3.2.4 HTTP/POST flood

A DDoS attack on the use of the IoT can pose a serious threat to the security of systems and networks. In these attacks, attackers infiltrate IoT devices and make them part of a zombie network (botnet). Then, with social coordination, these devices simultaneously send many requests to a specific target, usually using the HTTP protocol. These attacks can be performed as HTTP cascade attacks. In this type of attack, many HTTP requests are sent to the target server or service so that its resources are quickly maxed out and the server services are stopped. When the rate of session requests exceeds the number of valid users, server resources quickly run out. This malicious activity may lead to cascading DDoS attacks, for example, a cascading HTTP GET/POST attack. To perform this attack, the attacker needs a large, genuine HTTP request, and a botnet is usually used as a means of generating valid requests, typically sending more than 10 requests per second. This attack only requires one botnet to successfully launch an attack [60].

3.3 Network layer attacks

3.3.1 HELLO flood

In cognitive radio networks, the dissemination of Hello messages by nodes is done to establish node presence and exchange channel information. Nevertheless, the Hello Flood attack, an instance of malicious behavior, entails a node disseminating a powerful Hello message by a node to convince neighboring nodes that it belongs to their network. This results in rerouting all packets to the attacking node, resulting in their destruction. To illustrate, node M, the malicious entity in this example, sends a Hello message to node S to deceive it into thinking they are in a different area. As a result, node S, believing node M to be its neighbor, routes its packets to node M, thereby causing their loss Therefore, HELLO flood attacks can be problematic for IoT devices due to processing limitations, bandwidth consumption, weak security and inability to manage traffic, and act as a serious threat against these devices [61].

3.3.2 Sinkhole attack

Sinkhole attack is a type of DDoS attack that attracts traffic through a malicious node, causing a redirection of all traffic towards that node and, consequently, enabling further attacks on the system. In this attack, the attacker often gains unauthorized access to numerous devices such as computers, servers, or IoT devices to generate a large volume of malicious traffic. This traffic is subsequently directed to a network infrastructure known as a sinkhole, controlled by the defender. Therefore, sinkhole attack may be problematic for IoT devices due to resource limitations, communication disruption, weak security, impact on IoT services, and the risk of information theft and requires attention to the security of these devices.

Table 4 Comparison of techniques: SVM, K-means, PCA, KNN, random, forest, decision-tree

Diagnosis result	Advantages and disadvantages	Algorithm/model	DDoS detection technique
High accuracy—the fastest detection time and reduction of false positives	Advantages: Reduced detection time Improved performance Reduction in the number of features Disadvantages: High storage volume required Time consuming Algorithm complexity	PSO and ONE-SVM algorithms	ONE-SVM with PSO optimization [64]
Experimental designs yield higher accuracy, yet elevated loss function in some cases impairs detection accuracy	Advantages: Reduced complexity Improving the performance of the controller in the classification process Disadvantages: Longer training time of linear svm model	SVM algorithms	SVM-logistic regression coefficient [65]
Highly accurate attack detection, yet requiring multiple samples and varied conditions for comprehensive accuracy assessment	Advantages: Flexibility Using different variables Testing with actual data. Disadvantages: Requires training data Long training time Problem related to new attacks	Fuzzy algorithm's	Machine learning techniques, especially support vector machine (SVM), Fuzzy Tsukamoto [66]
It exhibits the best performance in terms of True Positive Rate (TPR), False Positive Rate (FPR), and the G-mean metric	Advantages: Reduced detection time Reduced feature count Adaptability to various device types. Disadvantages: The algorithm's complexity Need for large training samples Dependence on labeled data Lack of validation with newer datasets	GWO, OCSVM algorithms	Combination of two algorithms Gray Wolf Optimization and One Class Support Vector Machine to detect DDoS attacks [67]
Relatively high accuracy in detecting attacks	Advantages: Enhanced Performance via Parameter Optimization, Improved Data Quality, and Enhanced IoT Network Security. Disadvantages: Reliance on Training Data with Limited Impact on Attack Detection Accuracy	KNN	Machine learning with KNN algorithm [68]
The accuracy of detection relies on the model's performance. Increasing the number of features decreases accuracy but enhances the detection rate for various attacks	Advantages: Improved model performance Reduced computational complexity, enabling detection of various attacks Real-time analysis capability Disadvantages: Requires more data for model training Reduced accuracy with increasing dimensions Computational complexity in some cases	PCA, KNN	Dimensionality reduction algorithm and k-nearest neighbor classifier [69]

Table 4 (continued)

Diagnosis result	Advantages and disadvantages	Algorithm/model	DDoS detection technique
Reducing the number of centers in algorithms improves accuracy in classifying network traffic for both typical and DDoS attacks	Advantages: High efficiency in diagnosis Using meaningful features. Disadvantages: Requires labeled datasets Hybrid feature selection methods require experience and multiple tests Computational complexity	K-Means	K-Means clustering algorithm [70]
It provides a significant improvement in the accuracy of DDoS attack detection	Advantages: Reduced dependency on labeled data. Higher efficiency. Scalability to large datasets. Disadvantages Complex validation. Computational resource consumption	SKM-HFS	K-means semi-supervised algorithm using hybrid feature selection [71]
Relatively high accuracy percentage in detection	Advantages: Fast execution and energy saving High speed and efficiency in data processing Interpretability capability Feature selection. Disadvantages: Limitation of the domain It is not very accurate in detecting some attacks The need to process and select stronger features Prone to overfitting	Decision tree C4.5 algorithm	C4.5 decision tree for attack classification [72]
High precision in identifying attacks	Advantages: Improved system performance Enhanced data quality Disadvantages: Risk of over-removal using pearson correlation-based recursive feature elimination, resulting in potential loss of vital information and reduced model accuracy	DT-PCRFE algorithm	Using the decision tree method with Pearson correlation-based recursive feature removal mode [73]
High-precision real-time attack detection	Disadvantages: High computational processing. Threshold determination problems in using the Low Variance Filter technique in feature selection Advantages: Lowered resource usage due to the employment of a limited set of chosen features	Decision tree	The Lightweight Decision Tree Algorithm [74]
Accurate diagnosis, but limitations in feature selection may impact system diagnostic accuracy	Advantages:—Real-time attack detection—In-depth semantic interpretation and association rules Disadvantages: System complexity Requirement for suitable training data Limitations in detecting new attacks Resource consumption—Dependency on threshold values	Algorithm C4.5	C4.5 decision tree [75]

Table 4 (continued)

Diagnosis result	Advantages and disadvantages	Algorithm/model	DDoS detection technique
Optimal performance in accuracy	Advantages: Data complexity reduction achieved via sampling and feature selection Disadvantages: Choosing appropriate features Requires high computational resources Handling many features may require advanced data processing techniques	Random forest	Random Forest Algorithm to perform classification and attack detection techniques [76]
Enhances detection accuracy	Advantages: Simplified network design by eliminating a plethora of irrelevant characteristics Mitigates the problem of overfitting Disadvantages: Lack of interpretability confidence Streamlined network architecture by discarding a multitude of irrelevant features	Random forest	A combination of PSO and Random Forest [77]

3.3.3 Sybil attack

Sybil attack is a type of attack in which the attacker creates multiple fake identities or fraudulent nodes within a network to gain control over it or infiltrate it. That indicates that the attack originated from a multitude of sources. In the realm of DDoS attacks, a Sybil attack can amplify the impact of the assault, leading to increased resource depletion and a higher likelihood of disruption or service denial. Sybil attack is problematic and dangerous for IoT devices due to the allocation of names and resources, attack on security protocols, network interference, attack on decision-making systems, and security risk.

3.3.4 Wormhole attack

The aim of a Wormhole attack is to disrupt the network topology and traffic flow. A wormhole attack occurs when a malicious node tunnels messages between two distinct segments of the network through a high-speed link. This attack usually leads to the rerouting of data transmission and significant delays in the network. Wormhole attacks present significant challenges for IoT devices by compromising data integrity, misleading location information, disrupting routing, manipulating security protocols, causing resource exhaustion, challenging trustworthiness, and potentially leading to network partitioning. Mitigating these risks requires robust security measures and vigilance in the design and deployment of IoT systems.

3.4 Intrusion detection system

The unauthorized access to computers, which has become widespread across the internet, has emerged as a significant global threat. Researchers have proposed various methods, including firewalls and encryption, to prevent these breaches and protect computer systems. Despite these efforts, attackers have still managed to breach computer defenses. Intrusion Detection Systems play a crucial role by monitoring and reporting unusual activities, serving as a primary defense against hackers. These systems allow administrators to implement effective measures to block vulnerable ports, restrict access, and prevent future intrusions. IDSs come in various types, each with their advantages and disadvantages, tailored to the specific needs of the network. The intrusion detection techniques include signature-based IDS, anomaly-based IDS, and hybrid IDS. The structure of the intrusion detection system is shown in Fig. 4.

4 DDoS attack detection techniques in IoT: comparing methods

As shown in Fig. 5, DDoS attack detection techniques in IoT systems consist of three phases, each with its own unique strategies.

4.1 Signature-based DDoS attack detection model

In [62], The authors effectively tackled DDoS threats on network servers using SNORT, a signature-based intrusion

Table 5 Comparison of Logistic regression and Linear regression, XGboost, Gradient Boosting Machine, SOM, Back Propagation techniqu

Diagnosis result	Advantages and disadvantages	Algorithm/model	DDoS detection technique
It has high detection accuracy. This method can be Beneficial for detecting DDoS attacks, but some finer details may be lost	Advantages: Aiding in improving the model's performance Disadvantages: Need more computing resources Complexity of data preprocessing Accuracy alone is not enough in the evaluation metric for imbalanced data Generalizing of the model to DDOS attacks	Logistic regression	A PCA-based logistic regression model for classification [78]
Both LR and ANN methods have good results in detection accuracy, but ANN is slightly more accurate than some metrics	Advantages: Ability to model the complexity of data Disadvantages: Complexity and time-consuming Requires a large data set	Logistic regression algorithm	Feature extraction and classification with Logistic Regression, Artificial Neural Network [79]
LR initially has a lower accuracy and requires more training data to achieve higher accuracy	Advantages: High speed Disadvantages: Computational complexity Lower accuracy	Linear regression	Linear regression [80]
Reduced model accuracy Implementing consensus Based machine learning model using five days of traffic logs	Advantages: Provides insights into relationships between multiple attributes Enhancing Model Understanding. Disadvantages: Limited Analysis Reduced Accuracy. limited to a one-day log file	multiple linear regression analysis along with information gain-based feature selection	multiple linear regression [81]
Improved accuracy in attack detection, but lower accuracy in multi-class classification	Advantages: Improved intrusion detection performance and accuracy Disadvantages: Challenges in multiclass detection Requires a large amount of training data Requires precise configuration and selection of suitable parameters	Naive Bayes	Two-phase intrusion detection system using Naïve Bayes [82]
It has more efficiency and acceptable accuracy	Advantages: Multi-agent implementation Lower implementation cost. Disadvantages: Possibility of false positives Computational complexity	Naïve Bayesian algorithm	Simple Bayesian classification technique in multi-agent system [83]

Table 5 (continued)

Diagnosis result	Advantages and disadvantages	Algorithm/model	DDoS detection technique
High accuracy in detecting malicious traffic High sensitivity However, it has relatively low specificity	Advantages: Using the Dice Similarity Coefficient for data cleaning and better discrimination between feature patterns Reduction in the number of false alarms Disadvantages: Complexity of the method High false positive rate High fall-out rate	Naïve Bayesian algorithm	A distributed heterogeneous technique to optimize features to prevent intrusive activities [85]
The error rate is exceedingly low and has high accuracy	Advantages: Generalizability Accurate prediction Disadvantages: Need for precise configurations Complexity in setting High computational requirements	XGBoost	Effective intrusion detection using XGBoost [86]
Increasing accuracy in detecting attacks	Advantages: Flexibility in data segmentation Improved performance Disadvantages: Speed and time limit	Random Forest extreme Gradient Boosting	XGB-RF hybrid machine learning scheme [87]
Combined SOM model: Enhanced accuracy and efficiency, potential for further improvement	Disadvantages: Limitation of resources Complex implementation	k-nearest neighbor algorithm	A hybrid self-organizing map for attack detection [88]
Prediction accuracy, detection rate and performance accuracy are acceptable	Advantages: Reduced computational load Elimination of redundancies Dynamic forecasting Improved model performance High stability Disadvantages: Limitation when using a dataset that restricts result generalization High dependence on initial weights	Kalman backpropagation machine learning algorithm	Kalman Backpropagation Neural Network [89]
High detection accuracy and rate, low false positives/negatives; variations in performance between training and testing phases	Advantages: Resilience against attacks Reduced computational overhead Improved model accuracy. Disadvantages: Computational complexity Dependence on input data Consumption of computational resources Reliance on initial weights	Backpropagation	Neural network based on backtracking algorithm [90]

Table 6 Comparison of LSTM, GAN, CNN, RNN, MLP deep belief, statistical method techniques

Diagnosis result	Advantages and disadvantages	Algorithm/model	DDoS detection technique
High accuracy in detecting malicious traffic and normal traffic	Advantages: Accurate diagnostic capability Disadvantages: The need for a large data set Computational complexity Long training time -need to configure and set parameters	Convolutional Neural Network—CNN	Convolutional Neural Network – CNN [91]
High detection accuracy	Advantages: Improved detection accuracy.—Low processing cost Disadvantages: Requires training Complexity in hyperparameter tuning Dependency on network architecture features	Improved firefly algorithm	Improved Firefly Algorithm for Convolutional Neural Network Optimization [92]
It has high accuracy and good performance to detect new attacks. However, its detection accuracy is low for fresh attacks with less traffic	Advantages: The best method for detecting multiple attacks Significant improvement in accuracy Disadvantages: Training complexity and time-consuming Implementation complexity Its detection accuracy is lower for new attacks with less traffic	GAN-based algorithm	A GAN-based deep learning architecture for multiple attack detection [93]
Increasing the accuracy and ability to detect attacks	Advantages: Detection of random and composite attacks Generalizability Disadvantages: The accuracy and performance of this approach depend on the training data Training and configuring the GAN model can be time-consuming and complex	GAN-based algorithm	GAN based model [94]
It has higher performance, accuracy and f-score	Advantages: An effective method for analyzing time-based data Enhanced results with an increased time window Disadvantages: Precision and recall in the LSTM-BA model are not consistently higher than in the LSTM model Time-based detection accuracy on the fourth day is higher than on the fifth day	LSTM-BA	A combination of short-term and long-term memory and Bayes approach [95]

Table 6 (continued)

Diagnosis result	Advantages and disadvantages	Algorithm/model	DDoS detection technique
BCO-LSTM, optimized for LSTM parameters, outperforms traditional LSTM and some enhanced LSTM models in detecting DDoS attacks	Advantages:—Using BCO optimization Reducing the impact of personal experiences.—Convergence speed Disadvantages: Complexity of the text The need for training data to optimize the parameters. Data preprocessing may be time-consuming	BCO LSTM optimization algorithm	Using LSTM with BCO optimization algorithm [96]
Higher accuracy in detecting types of attacks	Advantages: Use of feature analysis Use of combined algorithms Disadvantages: Implementation complexity Complicated preprocessing Dependence on data	RNN algorithms	Detection and classification using Standardized Recurrent Neural Network [97]
It has higher accuracy and efficiency	Advantages: Using optimization techniques in feature selection The ability of the model to manage non-linear functions The flexibility of the model Disadvantages: Computational complexity The need to determine the province	Multilayer Perceptron Algorithm and Grid Search Algorithm	MLP model as a feed-forward neural network [98]
High accuracy in detecting attacks	Advantages: Features enhancements Performance improvement Ability to develop to detect types of attacks Disadvantages:—The need for limited calculations Complexity Time-consuming training The complexity of combining classes	Deep Belief Network algorithm	An Intrusion Detection System Based on Deep Learning Using Deep Belief Network Algorithm [99]

detection system. SNORT, an open-source tool, is logically divided into attack detection, threat identification, rule management, and development. Signature-based intrusion detection proves efficient for networks with fewer features, reducing modeling time. The system, comprising packet descriptors, preprocessors, detection engines, intrusion alert systems, and output modules, records network traffic with the Libecap library and separates data packets via a dedicated Ethernet card. SNORT inspects and evaluates data packets for network security, initiating pre-processing for detailed reports and alerts, facilitating comprehensive analysis and communication of findings.

In [63], intrusion detection systems using Blockchain signatures are employed to counter DDoS attacks. This signature-based system automatically updates rules and shares them with other network nodes, improving intrusion detection performance. Blockchain technology enables a focus on internal threats, enhancing overall network security against such threats.

Table 7 Comparison of SDN, FOG, smart contracts, Blockchain techniques

Diagnosis result	Advantages and disadvantages	Algorithm model	DDoS detection technique
Effective in detecting attacks, but challenges persist, including reducing false reports and improving detection rates	Disadvantages: Despite accurate attack detection, it generates some false reports Detection of coefficient changes require training and can be time-consuming Advantages: σ prediction tunnel for early attack detection Effectiveness in both real and simulated data	Hurst and autoregression coefficients and Variance of variation	One-Parameter Statistical Methods [100]
ARFIMA model had better detection rate (DR) and false positive (FP) values compared to the FIGARCH model	Advantages: Detect anomalies effectively in network traffic signal Disadvantages: not all traffic features were sufficient for detecting all simulated attacks	ARFIMA and FIGARH	Statistical autoregressive models for analyzing network traffic and detecting anomalies [101]
superiority of the proposed system with fewer I/O operations and faster execution	Advantages A Decentralized Paradigm for Enhanced Flexibility and Transaction Control Privacy and Security Enhancement Performance Improvement Prevention of future attacks Disadvantages: Scalability limitation Complexity Dependence on ethereum Limited evaluation aspects	Smart contract code and mentions six main functions	Ethereum blockchain and smart contracts [102]
It demonstrates a significant improvement in execution time and I/O operations, achieving faster performance	Advantages Enhanced security System resource management No need for hardware upgrades Disadvantages: Implementation complexity, Cost, intensive, Scalability limitations	Elliptic curves digital signature algorithm with, ecc digital signature algorithm	Ethereum, blockchain model [103]
It has a faster detection time and greater effectiveness	Advantages: The three-step strategy for enhancing overall efficiency Disadvantages: Requires more computational resources Requires more time to identify the attack traffic pattern, Detection of attacks based on threshold limits	Real-time traffic filtering algorithm	Fog calculations [104]
It has high accuracy in detection and a short time for identifying DDoS attacks. It has the capability to detect attacks in real-time	Advantages: Support for a variety of attacks, Use of Raspberry Pi, Utilization of entropy, No false positives, Real-time detection, High performance Disadvantages: Implementation complexity, Resource requirements, Model training is necessary	k-nearest neighbors	A hybrid fog computing approach [105]

Table 7 (continued)

Diagnosis result	Advantages and disadvantages	Algorithm model	DDoS detection technique
high accuracy	Advantages: Reduced latency, Low traffic, High transmission rate Disadvantages: Complexity, Resource requirements, Hardware resource dependency	Algorithm to analysis incoming packets	DDoS attack detection based on Fog layer [106]
High accuracy and low traffic cost	Advantages: Increased throughput capacity, Faster detection speed Disadvantages: High hardware resource requirements, need for updates to detect modified attacks Centralized control	Statistical analysis algorithms	Software defined network infrastructure [107]
It has high detection accuracy and an extremely low false positive rate	Advantages: Security management with SDN, Early detection, reduced false positives Disadvantages: System resource limitations, Need for updates, Possibility of false positives	Traffic generation, counter-based packet detection, payload-based detection, algorithms	SDN approach with time efficiency [108]
Empowering Io Security and Confidence with Blockchain Permissions and AI Contracts	Advantages: Increased security, access management, privacy assurance Disadvantages: Complexity, energy consumption, scalability, cost	Consensus algorithm	Smart contract design [109]

4.2 Anomaly-based detection models: machine learning classifiers

The framework of IDS based on machine learning is shown in Fig. 6.

4.2.1 SVM

In [64], the support vector machine algorithm is utilized for the detection and mitigation of DDoS attacks in IoT. It involves collecting network traffic data from IoT devices, extracting relevant features, preprocessing the features, and training the SVM model with labeled samples of normal and attack traffic. The performance is evaluated using labeled data, and the Particle Swarm Optimization algorithm (PSO) is employed for improved feature selection, reducing the time for attack detection. However, the text acknowledges that SVM alone may not be sufficient for identifying various types of DDoS attacks in IoT networks, suggesting the need for complementary approaches.

In [65], an intrusion detection system is developed to detect DDoS attacks using the SVM algorithm and feature importance method. The process involves building a classification model with SVM based on training data, utilizing logistic regression coefficients for feature selection, and

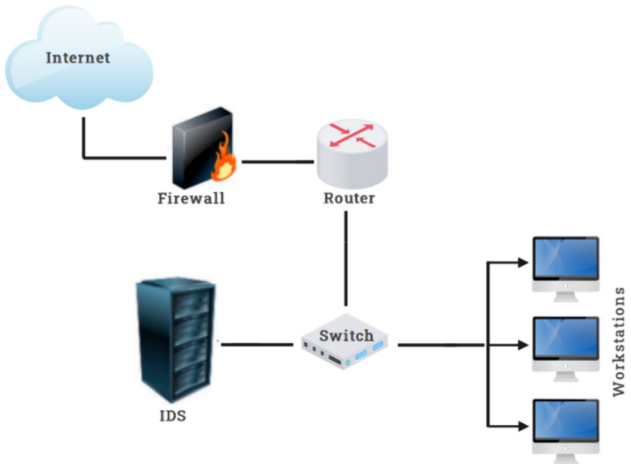

Fig. 4 Intrusion detection

conducting tests with test data sent to the SD-IoT switch. The switch processes the data, classifying packets as either DDoS attack or ordinary packets. The classification involves matching packet headers with the switch and distinguishing new packets, which are then sent for processing and classification using the SVM algorithm. Ordinary packets are identified as Ordinary flows, while DDoS packets trigger necessary actions to counter the LRDDoS

attack. The completed model is used for classifying DDoS and Ordinary packets in the IoT network.

In [66], two algorithms, Support Vector Machine and Tsukamoto Fuzzy, are used to identify DDoS attacks and evaluate classification performance. The Support Vector Machine method involves training the model with network traffic data, extracting features, and classifying traffic based on packet characteristics. Fuzzy variables are employed in conjunction with SVM to determine traffic types, allowing the system to detect DDoS attacks and recognize legitimate traffic.

In [67], DDoS attacks in IoT networks are identified using a novel approach. The One-Class Support Vector Machine (OCSVM) and Grey Wolf Optimization (GWO) algorithms are combined to detect both known and unknown attacks while preserving IoT device resources. The approach aims to increase detection accuracy, reduce false positives, increase true positives, and minimize selected features. The GWO-OCSVM model uses GWO's generation operators to balance exploration and exploitation, providing optimal hyperparameters and feature subsets. This approach not only detects DDoS attacks but also optimizes IoT device resource utilization, enhancing IoT network security.

4.2.2 K-nearest neighbors

In [68], machine learning and the KNN algorithm are utilized to detect and categorize network traffic data for malware attacks. The KNN algorithm, trained on attack and non-attack datasets, classifies new instances based on common attributes found in the attack data. The method involves data preparation, feature extraction, and Euclidean distance calculations. The parameter K, representing the number of nearest neighbors, is determined, and optimal features are selected for classification using the Gini index. The classification results are evaluated using confusion matrix calculation, and experiments measure the performance of the classification model.

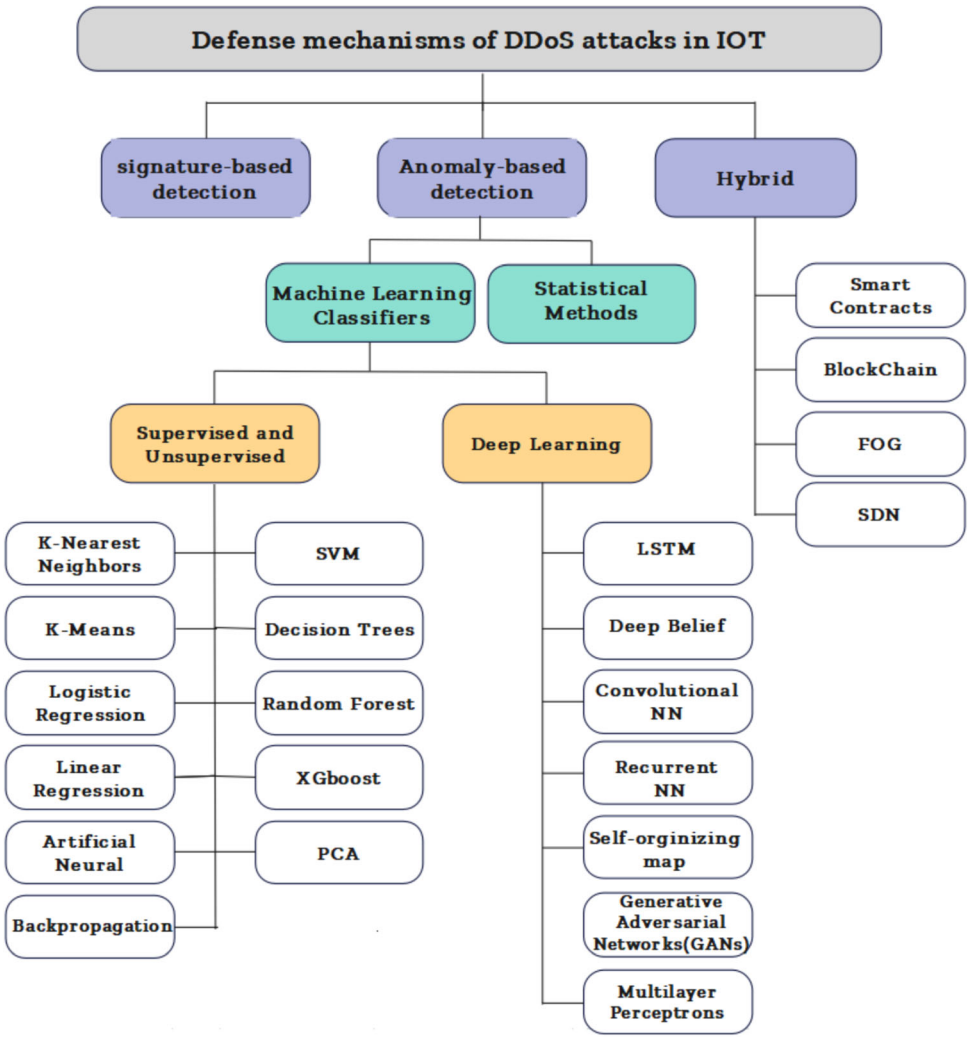

Fig. 5 DDoS Attack Detection Techniques in IoT

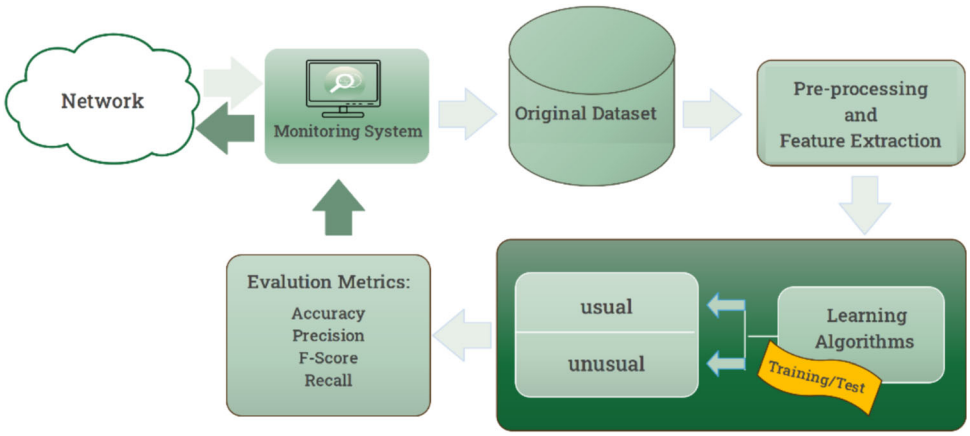

Fig. 6 General workflow of implementing an ML-based IDS model

4.2.3 PCA

In [69], the authors introduced an innovative intrusion detection model for IoT networks, employing principal component analysis for dimensionality reduction and combining softmax regression with k-nearest neighbor algorithms for classification. PCA extracts features, reducing their quantity, and the model uses softmax regression and K-NN for distinguishing between normal and malicious behaviors in IoT networks. Softmax regression handles multiple classes, employing predefined functions to calculate attack class probabilities, while K-NN classifies objects based on nearest neighbors' votes. The combined use of PCA, softmax regression, and K-NN enables effective and accurate detection of malicious intrusions in IoT networks.

4.2.4 K-means

In [70], the utilization of the K-Means clustering algorithm is introduced as a machine learning approach for identifying DDoS attacks in networks and anomalous traffic. The methodology involves separating regular and irregular traffic using the K-Means algorithm, assigning cluster names based on shared statistical features. The Canopy method is employed as a preprocessing step, and feature selection is enhanced using variance filtering and information gain techniques. Variance filtering discards low-variance features, while information gain assigns weights based on feature importance. These techniques improve the accuracy of DDoS attack detection in the K-Means algorithm by selecting valuable features and removing irrelevant ones.

In [71], an intrusion detection framework involves preparing, preprocessing, and selecting significant features using the SKM-HFS hybrid method. The K-means algorithm splits the dataset into Typical and DDoS attack clusters. A three-step feature selection method, including normalization, ranking, and subset search, efficiently analyzes data. Entropy measures the randomness of network traffic, aiding DDoS attack detection. The framework uses k-means sum-squared error filtering for feature selection ranking and a sequential forward selection algorithm to find the best feature subset for the detection model. Detection performance is evaluated using multiple metrics.

4.2.5 Decision trees

In [72], the C4.5 decision tree algorithm is employed as a classification tool for DDoS attack detection, utilizing data gathered from network traffic generators. The algorithm predicts labels through classification, categorizing new data based on predefined class labels for DDoS attack detection. The process involves data collection, division into training and testing sets, and analysis of network traffic features. Feature selection employs the Pearson correlation coefficient to identify those strongly correlated with the target class. Selected features are integrated into the classification model, where the algorithm uses the gain ratio to determine the best features for decision-making within a tree structure. The decision tree enhances DDoS attack detection accuracy by learning patterns from training data and applying them to predict labels for new, unseen data.

In [73], a DDoS attack detection system model for IoT comprises four steps: preprocessing, feature selection, feature combination, and attack detection classification. Preprocessing involves data cleaning and normalization using hot encoding. Feature selection uses Pearson Correlation Recursive Feature Elimination and decision tree-based methods. Features are combined, and weight values are determined. A Deep Neural Network classifier then identifies patterns in malicious DDoS requests on IoT devices, distinguishing them from typical requests.

In [74], a lightweight neural network approach is used for attack detection, employing a monitoring system across multiple host machines or network devices. The system,

executed through port mirroring, provides flexibility and resilience. Features related to DDoS attacks are extracted through pre-processing, and low-variance feature selection highlights relevant features. Data is normalized using min–max normalization, and a Decision-Tree model learns patterns for classifying network traffic into regular or DDoS attack categories. The model is then tested on validation data to assess DDoS attack detection accuracy.

In [75], the C4.5 algorithm and association rules are used to detect and analyze traffic flood attacks. The Correlation-based Feature Selection method selects crucial features, and probabilistic models assess attack likelihood based on nominal features. Entropy measures uncertainty, automatic rule extraction and deep semantic interpretation methods identify patterns, enabling the categorization of traffic flood attacks. The approach is effective in detecting and analyzing such attacks through the exploration of association rules.

4.2.6 Random forest

In [76], random forest, a machine learning method, is employed to identify and classify network traffic in four main stages. It involves collecting data from various sources, organizing it based on performance and data collection type, and specifying time frames for data intervals. The collected data undergoes processing, combining normal and attack traffic and employing sampling for dimension reduction. Essential features are then selected to distinguish benign traffic from malicious traffic, and a model is created for recognizing and classifying normal and attack traffic using the Random Forest algorithm.

In [77], a novel approach enhances DDoS attack detection using the fusion of Random Forest Optimization and Particle Swarm Optimization. The PSO algorithm generates relevant attributes for distinguishing between Normal and attack traffic in IoT. Optimized features are then applied to the Random Forest classification algorithm, forming an ensemble of decision trees. The algorithm's performance is evaluated through various classification tests, such as hold-out and cross-validation, to determine its accuracy in detecting Normal and attack traffic.

4.2.7 Logistic regression

In [78], a method for classifying and identifying DDoS attacks using a logistic regression model based on principal component analysis is introduced. The process involves initial data preprocessing, including removal of incorrect and duplicate entries, division of data into training and testing sets, standard scaling for normalization, PCA for dimensionality reduction, model evaluation, and training using logistic regression. The final models are evaluated on an updated test set to assess their effectiveness in DDoS attack detection. The approach combines standard scaling, PCA-based dimensionality reduction, and logistic regression to improve the precision of DDoS attack detection.

In [79], logistic regression is employed to extract crucial features for classifying and detecting DDoS attacks in the IoT. The approach selects a subset of features with the most information and significance, improving the accuracy of category classification. The logistic regression model adjusts weights associated with attributes, minimizing less important features. Features are sorted based on weights, and the most significant feature is selected. The model calculates the probability of each sample belonging to categories using the sigmoid function. Samples are then classified as Normal data or DDoS attack based on a decision threshold, facilitating accurate classification.

4.2.8 Linear regression

In [80], A framework is used to detect DDoS attacks using machine learning and linear regression methods. The framework comprises five main steps: dataset selection, tool and language selection, data preprocessing, data encoding, and data partitioning. Finally, the data partitioning stage divides the data into two sets: training and testing, for model creation and performance evaluation. A linear regression algorithm is employed to classify data, and the final output, indicating the occurrence of a DDoS attack, is determined as binary (0 or 1) through a binary step function.

In [81], DDoS attack detection using the CICIDS 2017 dataset is performed using multiple linear regression and information augmentation-based feature selection. The model achieves 73.79% accuracy in predicting DDoS attacks from Friday afternoon log files, demonstrating the importance of regression analysis and visualizations such as goodness-of-fit and residual plots.

4.2.9 Naïve Bayes

In [82], a two-stage intrusion detection system is presented, combining a Naive Bayes classifier and an unsupervised elliptic overlay for attack detection. The first stage classifies data into four sections using Naive Bayes, with results determined through majority voting. The second stage refines classification using the unsupervised "ellipse coverage" method. Data preprocessing involves analysis, transformation, and feature selection techniques. Weight assignment is crucial for accurate predictions, especially in imbalanced label distributions, with weight computations and predicted values distinguishing between intrusive and normal behaviors.

In [83], the Naïve Bayes classification algorithm is applied to intrusion detection systems for safeguarding IoT infrastructure against DDoS attacks. The algorithm utilizes Bayes theorem for event probability calculation and operates in three stages: data classification, preprocessing with feature and sample removal, and test data classification. The Intrusion Detection System involves four agent types: Collection, System Monitoring, Triggering [4], and Communication Agents within a Multi-Agent System [84], facilitating distributed load distribution for rapid attack detection and prevention reporting.

In [85], the Naive Bayes method is utilized for enhancing IoT network security as an intrusion prevention system capable of detecting and responding to dynamic DDoS attacks. The approach involves training a model on labeled network transaction data to identify unique feature subsets, utilizing the Dice similarity coefficient for pattern distance measurement. Feature selection is performed through the correlation coefficient approach, and the selected features are used to train a Naive Bayes classifier, improving IoT network security against diverse attacks.

4.2.10 XGboost

In [86], XGBoost, a tree-based machine learning algorithm, is discussed to build a robust intrusion detection system. This algorithm can detect and distinguishing between different data categories by making critical decisions based on dataset features. The algorithm partitions the dataset into branches, with features treated as conditional nodes, and builds a tree for decision-making. The objective function includes training loss and regularization, aiming to minimize errors and control model complexity. XGBoost optimizes learned trees sequentially, adding new decision trees to improve prediction accuracy and overall model performance. The algorithm is particularly suitable for complex problems like prediction, classification, and ranking.

In [87], a combined machine learning approach called XGB-RF is proposed for IoT intrusion attack detection. This method uses Random Forest for feature selection and XGBoost for intrusion detection, addressing imbalanced datasets through MIN–MAX scaling. Various feature selection methods, including Recursive Feature Elimination, Recursive Feature Elimination with Cross-Validation, and Select-K-Best with RF-based features, are applied. Random Forest efficiently selects features based on criteria like Gini and average accuracy reduction, preventing overfitting. XGBoost optimizes error functions for attack detection, and the final model is selected based on a threshold for the difference between machine estimates and actual data.

4.2.11 Self-organizing map

In [88], a hybrid model for DDoS attack detection is introduced, which combines a self-organizing map (SOM) with a supervised artificial neural network. The SOM enhances prediction accuracy using the K-Nearest Neighbor algorithm, and the training dataset focuses on IoT botnet attacks. Preprocessing involves scaling, transforming, and encoding input data with labeled features. Overfitting is addressed using the Sklearn Extra Trees classifier. After preprocessing, deep learning models are trained through supervised and semi-supervised methods on labeled datasets to distinguish between normal and malicious traffic. The approach aims to improve DDoS attack detection accuracy through the integration of SOM, neural networks, and preprocessing techniques.

4.2.12 Back propagation

In [89], the Kalman backpropagation neural network is used as an intelligent intrusion detection mechanism against DDoS attacks in IoT. The model comprises four stages: Dataset Source, Dataset Pre-processing, DDoS Classification, and Evaluation and Scoring. The advanced backpropagation neural network is enhanced using a Kalman filter for improved performance. The dataset is collected, organized, and normalized using the min–max method. The Kalman backpropagation neural network is then employed in the DDoS classification stage, utilizing forward propagation and backpropagation during training. The Evaluation and Scoring stage assess the model's effectiveness in detecting DDoS attacks based on network outputs for each layer.

In [90], an intelligent intrusion detection model based on a back-propagation neural network is employed to detect DDoS attacks in IoT networks. The model involves a recursive process with forward and backward phases, using a real-world dataset that undergoes preprocessing steps such as cleaning, feature selection, and normalization. The trained feedforward neural network serves as a smart intrusion detection system, capable of distinguishing between DDoS attack and normal traffic in new streams and triggering alert notifications.

4.2.13 CNN

In [91], the use of Convolutional Neural Network to classify normal traffic and DDoS attacks is discussed in three main steps. The training phase utilizes a combination of online and offline datasets, with the online dataset capturing real-time traffic and the offline dataset containing normal and malicious traffic. Feature extraction involves parameters such as reception time, time differences,

addresses, ports, protocol, and TCP flags. Each row is transformed into a 3 × 3 matrix treated as a 2D image, and the pooling layer reduces matrix size. In the classification step, the model is trained, and the fully connected layer produces a one-dimensional array representing classes (Normal or DDoS attack).

In [92], an improved CNN model named IFACNN is employed for detecting DDoS attacks in the IoT environment. The model consists of four stages: collecting header information from IoT switches, preprocessing data packets, extracting features from network streams, and detecting DDoS attacks using the IFACNN neural network. A custom module sends packet collection commands to IoT switches, ensuring a rapid response to DDoS attacks. The preprocessing stage categorizes data packets based on similar quintuples and distributes them to different network streams. Features of network streams are then extracted for input into the deep learning algorithm, aiming to detect DDoS attacks. The IFACNN neural network is employed for precise detection, and network parameters are finely tuned using the "Firefly Algorithm" for optimal performance.

4.2.14 GAN

In [93], a Generative Adversarial Network (GAN) is employed for Network Intrusion Detection. The GAN consists of a discriminator and a generator, creating new data samples resembling network traffic patterns to challenge the discriminator. The intrusion detection model involves feature extraction using Ensemble Mutual Information Feature Selection, optimizing the model to detect novel attacks. The GAN-based approach exhibits higher accuracy and fewer false positives, particularly effective in detecting new attacks.

In [94], a Generative Adversarial Network (GAN) framework enhances DDoS attack detection. It employs a deep neural network classifier distinguishing between DDoS and non-malicious samples. Two models generate artificial traffic instances, with the classifier trained to detect DDoS by modifying non-malicious features. Preprocessing adjusts labels for UDP-based DDoS, removes specific features, and normalizes data. The approach includes a detection model and two generators. The classifier, trained with high accuracy, is tested, demonstrating accurate predictions, and is retrained with higher weight on attack features, effectively distinguishing between attack and benign data.

4.2.15 LSTM

In [95], a hybrid method named LSTM-BA is introduced for enhancing DDoS attack detection in networks. This method combines the LSTM network and Bayesian approach, where LSTM identifies attacks, and if predictions are unsatisfactory, the data moves to the Bayesian module for further analysis. The final output is a combination of outputs from both modules, with the LSTM network utilizing a recurrent cell chain for understanding temporal data. Traffic classification uses values below 0.5 for Normal and above 0.5 for Attack. The Bayes module improves probability assessment, reducing false detections and triggering alerts if an attack is detected.

In [96], a more efficient method for detecting DDoS attacks is introduced, combining the LSTM algorithm with Bacterial Colony Optimization (BCO). The BCO optimization algorithm is employed to optimize LSTM parameters, aiming to increase the detection rate by obtaining optimal parameters and improving performance in terms of detection rate and convergence speed with high accuracy. The BCO-LSTM approach involves setting parameters, normalizing input data, dividing data into training and test sets, optimizing LSTM parameters using BCO, recording the best parameters, and evaluating the trained model for DDoS attack detection.

4.2.16 RNN

In [97], a Recurrent Neural Network (RNN) is employed for network intrusion detection, involving stages such as data collection, preprocessing, neural network modeling, and training with three different algorithms. Data collection includes gathering information for RNN training, focusing on connection attacks and intrusions. In the preprocessing stage, collected data is processed, irrelevant information is removed, and labels are assigned. The RNN is trained using gradient descent, scaled conjugate gradient, and variable learning rate algorithms, fine-tuning weights and parameters for enhanced network performance. The trained model is then used to classify incoming traffic.

4.2.17 MLP

In [98], a dynamic MLP-based method for DDoS attack detection is presented with three modules: the knowledge base, detection model, and feedback mechanism. The knowledge base maintains labeled training and feedback datasets, while preprocessing converts samples for the detection model. The model employs an MLP classifier with SBS feature selection. The feedback mechanism updates the knowledge base, reconstructs the model, and improves accuracy. When the feedback dataset surpasses a threshold, the mechanism is activated, and errors are reported for model updates, proving effective against evolving attacks.

4.2.18 Deep Belief

In [99], the Deep Belief Network algorithm, a deep learning approach, is applied to Intrusion Detection Systems. The DBN utilizes a layer-by-layer methodology, where each layer serves as a Restricted Boltzmann Machine (RBM) model trained on the previous layer. The DBN is initially composed of RBM layers during pre-training, followed by fine-tuning using a Feedforward Neural Network. Techniques like RBM and auto-encoders enhance model performance, especially in scenarios with limited labeled data. The training is done incrementally, optimizing each layer sequentially, followed by a fine-tuning phase with a combined supervised training algorithm.

4.3 Statistical methods

In [100], three single-parameter statistical methods (Hurst coefficients, autocorrelation, and change coefficient) are employed for DDoS attack detection in networks. The methods use 'acceptable' and 'critical' regions of parameter values to distinguish between valid network traffic and potential attacks. Standard datasets aid in determining value ranges for parameters, categorized as 'acceptable' or 'critical,' without requiring prior learning. Statistical methods, including the Hurst exponent, autoregression coefficient, and variance coefficient, are used to identify patterns and changes in data. A novel method, 'Sigma Tunnel Prediction,' is introduced for early attack diagnosis, demonstrating the effectiveness of univariate statistical approaches in enhancing early DDoS detection.

In [101], statistical autoregression models, namely ARFIMA and FIGARCH, are employed for DDoS attack detection in network traffic. The ARFIMA model estimates and predicts variable and changeable network traffic patterns with sparse parameterization, chosen based on information criteria. The FIGARCH model analyzes and predicts temporal characteristics, describing long-memory in variance series through maximum likelihood estimation. Both models contribute to modeling parameter variability in time series, crucial for detecting anomalies or attacks by comparing estimated and actual network traffic factors.

4.4 Hybrid detection models

4.4.1 Blockchain

In [102], a model is presented that utilizes the Ethereum blockchain to combat DDoS attacks in IoT systems. This model employs Ethereum as a public platform and Ether cryptocurrency for financial transactions and executing artificial intelligence contracts. The system incorporates various security measures, including assigning group IDs to IoT devices, validating device IDs against a whitelist, and monitoring gas limits for transactions to prevent unspecified attacks. Additionally, the system regularly monitors device behavior, removing unknown and malicious devices from the whitelist. These measures collectively enhance the security and trust of the IoT network against DDoS attacks.

In [103], the authors presented an Ethereum blockchain model as a solution to detect and prevent DDoS attacks against IoT systems. In addition, the suggested system can be employed to solve duty points (dependency on third parties) and maintain privacy and security in IoT systems. Initially, the plan is to execute a decentralized platform at the application layer to authenticate and verify these devices instead of the current centralized solutions to prevent DDoS attacks on IoT devices. In the second step, it is suggested that the IP address of the malicious devices be tracked and recorded in the blockchain to prevent their connection and communication with the IoT.

4.4.2 Fog computing

In [104], a method for mitigating DDoS attacks is introduced, employing edge computing. This approach expands local network edge computing services through a three-tier architecture: field-level, local-level, and cloud-level analysis of malicious network behaviors. At the field level, monitoring tools such as firewalls regulate network traffic to prevent botnet attacks. The local level uses computational resources at the network edge for DDoS attack analysis and mitigation. Detected attacks are forwarded to the cloud level for further analysis and countermeasures, utilizing distributed computing functions to combat DDoS attacks effectively.

In [105], a fog computing framework is proposed for real-time DDoS attack detection and mitigation, focusing on proximity to IoT devices. The system comprises IoT and fog layers, where sensor data is collected, preprocessed, and encrypted for standardized extraction. The fog layer analyzes real-time data using tools like Wireshark, applying entropy and the KNN algorithm for DDoS attack detection. Detected attack source IP addresses are added to a real-time blacklist for mitigation.

In [106], the proposed approach for DDoS attack detection employs Fog Computing, focusing on Normal traffic modeling to identify anomalies as potential attacks. The system has two layers: IoT devices and fog computing, where data is collected, processed, and sent to a cloud server. Malicious IoT devices are identified by analyzing data traffic through the fog node, utilizing entropy changes to measure randomness. The detection is based on identifying similar malware installations on IoT devices,

comparing entropy values with a defined threshold to detect DDoS attacks.

4.4.3 SDN

In [107], Software-Defined Networking (SDN) is praised for its ability to identify and counter DDoS attacks using features like software-based traffic analysis and centralized control. SDN controllers, powered by AI algorithms, detect abnormal traffic behavior and prevent potential threats. The DDoS identification process involves requesting flow statistics, extracting features, and using classifiers like Self-Organizing Maps to distinguish legitimate traffic from attacks. SDN deployment enables collaborative information exchange between domains, making it easier to trace and manage network attacks, including those from IoT devices.

In [108], a secure IoT framework is proposed, leveraging Software-Defined Networking (SDN) for vulnerability identification and malicious traffic detection. The framework, implemented on an SDN controller, employs IP session counters and payload analysis for threat detection, with a focus on DDoS attacks in SD-IoT networks. It features both countermeasure-based and load-based detection modules, continuously monitoring logs and analyzing traffic sizes to detect DDoS attacks. The dual approach enhances the controller's decision-making capabilities to counteract network changes, leveraging packet payload sizes to differentiate between legitimate and malicious packets, considering that DDoS attacks often involve bots exploiting vulnerabilities and using preloaded scripts to generate and transmit packets.

4.4.4 Smart contracts

In [109], a system utilizing intelligent contracts on the Hyperledger Fabric network is designed to enhance security and privacy in IoT systems. Smart contracts assess security risks related to IoT events, manage access permissions, and use network channels to bolster system security and privacy. The system includes an IoT prototype with image sensors for visitor management. Smart contracts follow predefined conditions in the ledger, flagging suspicious transactions and issuing warnings for violations. The combination of AI contracts, document immutability, and blockchain certificates ensures secure handling of personal data against network attacks. In summary, the system employs blockchain and smart contracts to improve security and privacy in IoT communications.

5 Challenges, open issues and opportunities

Detecting DDoS attacks in the context of the IoT presents several challenges, open issues, and opportunities. In conclusion, DDoS attack detection in IoT is a complex and evolving field. While it presents numerous challenges and open issues, it also offers opportunities for innovation in the realms of machine learning, behavioral analysis, and collaborative defense. Due to the discussions, we engaged in regarding diverse solutions to prevent DDoS attacks, our primary concentration is on developing innovative approaches, and enhancing security mechanisms to detect and deal with DDoS attacks in IoT. To defend against DDoS attacks in IoT networks, we encountered challenges that are discussed in this section. In this section, we intend to present the challenges and limitations in detecting and mitigating DDoS strategies. In the end, we will provide various and optimal defense solutions to ensure security against DDoS attacks in the future. Here are some key considerations:

5.1 Challenges

Scalability in IoT security One of the fundamental difficulties of the investigated methods was the scalability challenge in the field of managing DDoS attack detection systems in IoT The main question was how to scale these systems to adapt to the increasing traffic from IoT devices.

Resource constraints IoT devices typically have limited computing power, memory, and network bandwidth, making it challenging to implement sophisticated DDoS detection mechanisms.

Diverse device types IoT encompasses a wide range of devices with different capabilities and communication protocols. Detecting attacks across this diversity can be complex.

Traffic variability IoT devices generate traffic patterns that can be highly variable, making it difficult to distinguish normal behavior from malicious traffic.

Attack sophistication DDoS attacks are evolving and becoming more sophisticated. Attackers can use IoT devices to launch multi-vector attacks, making detection more challenging.

Data volume The sheer volume of data generated by IoT devices can overwhelm traditional detection systems, requiring scalable solutions.

Efficiency of energy consumption Considering the energy limitations of IoT devices, future guidelines should consider the ability to reduce the energy consumption of DDoS attack detection and valid security measures within these limitations.

Computational complexity Computational complexity in detecting DDoS attacks is one of the main challenges in the security of networks and the IoT. DDoS attacks usually try to overwhelm a target by sending an enormous quantity of traffic to render it.

5.2 Open issues

*Anomaly detection*Developing effective anomaly detection models for IoT traffic is an ongoing challenge. IoT networks have unique behavior patterns that may not align with traditional network traffic.

False positives Reducing false positives is crucial in IoT DDoS detection. Traditional detection methods may not work well, as IoT traffic can exhibit unpredictable patterns.

Privacy concerns IoT devices often collect sensitive data. Balancing security with privacy is an open issue, as monitoring traffic to detect attacks may raise privacy concerns [110].

IoT device heterogeneity The diversity of IoT devices complicates the development of standardized detection approaches. Each device type may require a tailored solution.

Real-time detection DDoS attacks require quick responses. Real-time detection and mitigation in IoT environments are challenging due to resource constraints.

5.3 Opportunities

*Machine learning*Utilizing models based on artificial intelligence in IoT security and DDoS attack detection has been used as scalable solutions [111]. These models can improve the accuracy of DDoS detection on the IoT and adapt to evolving attack patterns [112]. However, these models still need further development and optimization to best deal with the challenges in IoT security and DDoS attack detection.

Behavioral analysis Analyzing the behavior of IoT devices over time can help identify anomalies and potential attacks.

Edge computing Employing edge computing for DDoS detection can reduce the reliance on centralized resources and enhance real-time detection capabilities.

Collaborative defense IoT devices can work together to detect and mitigate DDoS attacks. A collaborative defense approach can distribute the detection workload.

IoT security standards The development of industry wide IoT security standards can help address some of the open issues. Standardized security practices can enhance DDoS detection.

IoT security awareness Raising awareness among IoT device manufacturers and users about the importance of security can lead to better-designed devices and networks less susceptible to DDoS attacks [113].

Therefore, artificial intelligence solutions align well with the current security needs of the IoT. Machine learning-based defense models can effectively deal with even Internet vulnerabilities due to their accurate ability to identify and predict millions of network intrusions compared to other defense mechanisms, also enhance the effectiveness and precision of detecting and predicting DDoS attacks. Models using machine learning techniques can extract diverse and complex features from network data and accurately identify and classify attacks using classification algorithms. Furthermore, these defense models are flexible and updatable and can adapt and perform better in response to changes in the type and severity of attacks. However, many machine learning-based methods have not addressed essential requirements for identity verification and authentication of IoT nodes. From a detection methods perspective, comparative evaluations have led us to the deduction that artificial intelligence approaches can be the best choice. Nevertheless, it should be noted that these results are not definitive.

6 Examining article criticisms and proposed criteria

To evaluate these articles and choose a criterion based on specific criteria, the following points can be considered:

Detection accuracy: Evaluation of attack detection accuracy based on each algorithm.

Time efficiency: A study on the speed of detection and reduction of the number of errors may be useful in this case.

Generalizability: Evaluating the applicability of algorithms to different environments and problems.

Resource consumption: Amount of memory and time consumption by algorithms.

Application in IoT networks: Application in IoT networks: Investigating the ability of algorithms to detect attacks in IoT networks.

6.1 The idea of presenting criteria:

Flexibility criterion: Evaluating the flexibility of algorithms in detecting new attacks and adapting to different conditions. Investigating Exploring the ability of algorithms to integrate with other methods to improve performance. This criterion, because flexibility is paramount in addressing the ever-changing landscape of threats in the field of network security, can lead to a better evaluation of algorithms.

7 Conclusion

In this comprehensive research review, we've explored various aspects of defending against DDoS attacks on the IoT. This review has been done through a detailed classification of different defense mechanisms. The main objective of this review is to offer thorough comparative analyses of all defense mechanisms, with an emphasis on the system models that are employed. Each article's defense architecture focuses on different aspects of DDoS attack detection and mitigation, providing valuable insights and solutions to address the challenges posed by DDoS attacks. Traditional approaches of intrusion detection mechanisms have limitations and problems and cannot deal with new and changing challenges in the domain of network security alone. The need for cleverer methods based on machine learning and deep learning is felt in the context of intrusion detection and identification of new and unknown attacks. Consequently, the integration of cutting-edge artificial intelligence techniques can significantly elevate the precision and efficiency of detecting network intrusions and fortifying network security. The introduced techniques still do not provide a complete response to all types of attacks and technologies related to IoT. These techniques have undergone thorough review to identify their weaknesses against DDoS attacks.

Author contributions Author Contributions The first draft of the manuscript was written by Amir Pakmehr and all authors commented on previous versions of the manuscript. Amir Pakmehr: Conceived and designed the analysis; contributed to the writing of the manuscript; critically reviewed the manuscript. Andreas Aßmuth: Contributed to the design and implementation of the research; contributed to the analysis of the results; assisted in the writing of the manuscript. Negar Taheri: Participated in the writing and editing of the manuscript. Ali Ghaffari*: Oversaw the project direction and planning; contributed to the critical revision of the manuscript for important intellectual content; acted as the corresponding author. *Correspondence: Ali Ghaffari (a.ghafari@iaut.ac.ir)

Funding Open access funding provided by the Scientific and Technological Research Council of Türkiye (TÜBİTAK). The authors have not disclosed any funding.

Data availability The authors do not have permission to share data.

Declarations

Competing interest The authors declare no competing interests.

References

1. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., Ayyash, M.: Internet of things: a survey on enabling technologies, protocols, and applications. IEEE Commun. Surv. Tutor. **17**(4), 2347–2376 (2015)
2. Cheng, B., Zhu, D., Zhao, S., Chen, J.: Situation-aware IoT service coordination using the event-driven SOA paradigm. IEEE Trans. Netw. Serv. Manage. **13**(2), 349–361 (2016)
3. Shukla, P., Krishna, C.R., Patil, N.V.: EIoT-DDoS: embedded classification approach for IoT traffic-based DDoS attacks. Clust. Comput. **27**(2), 1471–1490 (2024)
4. Fu, X., Pace, P., Aloi, G., Guerrieri, A., Li, W., Fortino, G.: Tolerance analysis of cyber-manufacturing systems to cascading failures. ACM Trans. Internet Technol. **23**(4), 1–23 (2023)
5. Roman, R., Zhou, J., Lopez, J.: On the features and challenges of security and privacy in distributed internet of things. Comput. Netw. **57**(10), 2266–2279 (2013)
6. D. Zhou, M. Sheng, C. Bao, Q. Hao, S. Ji, and J. Li, 6G Non-terrestrial networks-enhanced IoT service coverage: Injecting New vitality into ecological surveillance. IEEE Network, 2024.
7. Aguru, A.D., Erukala, S.B.: A lightweight multi-vector DDoS detection framework for IoT-enabled mobile health informatics systems using deep learning. Inf. Sci. **662**, 120209 (2024)
8. Jiang, H., Xiao, Z., Li, Z., Xu, J., Zeng, F., Wang, D.: An energy-efficient framework for internet of things underlaying heterogeneous small cell networks. IEEE Trans. Mob. Comput. **21**(1), 31–43 (2020)
9. Cao, B., Wang, X., Zhang, W., Song, H., Lv, Z.: A many-objective optimization model of industrial internet of things based on private blockchain. IEEE Netw. **34**(5), 78–83 (2020)
10. Liu, C., Xie, K., Wu, T., Ma, C., Ma, T.: Distributed neural tensor completion for network monitoring data recovery. Inform. Sci. **4**, 120259 (2024)
11. Dibaei, M., Ghaffari, A.: Full-duplex medium access control protocols in wireless networks: a survey. Wirel. Netw. **26**(4), 2825–2843 (2020)
12. Ghaffari, A.: Designing a wireless sensor network for ocean status notification system. Indian J. Sci. Technol. **4**, 809–814 (2014)
13. Stankovic, J.A.: Research directions for the internet of things. IEEE Internet Things J. **1**(1), 3–9 (2014)
14. Y. Liu et al. SS-DID: a secure and scalable Web3 decentralized identity utilizing multi-layer sharding blockchain. In: *IEEE Internet of Things Journal*, 2024.
15. W. Li, W. Susilo, C. Xia, L. Huang, F. Guo, and T. Wang, Secure data integrity check based on verified public key encryption with equality test for multi-cloud storage. In: IEEE Transactions on Dependable and Secure Computing, 2024.
16. Saiyed, M.F., Al-Anbagi, I.: A genetic algorithm-and t-test-based system for DDoS attack detection in IoT networks. IEEE Access **12**, 25623–25641 (2024)
17. Akhbari, A., Ghaffari, A.: Selfish node detection based on fuzzy logic and Harris hawks optimization algorithm in IoT networks. Secur. Commun. Netw. **2021**(1), 2658272 (2021)

18. Mohammadi, R., Akleylek, S., Ghaffari, A.: SDN-IoT: SDN-based efficient clustering scheme for IoT using improved Sailfish optimization algorithm. PeerJ Comput. Sci. **9**, e1424 (2023)
19. Salehnia, T., et al.: An optimal task scheduling method in IoT-Fog-Cloud network using multi-objective moth-flame algorithm. Multimedia Tools Appl. **83**(12), 34351–34372 (2024)
20. Seyfollahi, A., Mainuddin, M., Taami, T., Ghaffari, A.: RM-RPL: reliable mobility management framework for RPL-based IoT systems. Clust. Comput. **4**, 20–21 (2023)
21. Seyfollahi, A., Moodi, M., Ghaffari, A.: MFO-RPL: a secure RPL-based routing protocol utilizing moth-flame optimizer for the IoT applications. Comput. Standards Interfaces **82**, 103622 (2022)
22. Srivastava, A., Gupta, S., Quamara, M., Chaudhary, P., Aski, V.J.: Future IoT-enabled threats and vulnerabilities: State of the art, challenges, and future prospects. Int. J. Commun. Syst. **33**(12), e4443 (2020)
23. Kaushal, R.: Bitcoin: vulnerabilities and attacks. Imp. J. Interdiscip. Res. **2**(7), 944–946 (2016)
24. Shukla, P., Krishna, C.R., Patil, N.V.: SDDA-IoT: storm-based distributed detection approach for IoT network traffic-based DDoS attacks. Clust. Comput. **24**, 1–28 (2024)
25. Kumari, P., Jain, A.K.: Timely detection of DDoS attacks in IoT with dimensionality reduction. Clust. Comput. **41**, 1–19 (2024)
26. Román-Castro, R., López, J., Gritzalis, S.: Evolution and trends in IoT security. Computer **51**(7), 16–25 (2018)
27. Asgharzadeh, H., Ghaffari, A., Masdari, M., Gharehchopogh, F.S.: Anomaly-based intrusion detection system in the Internet of Things using a convolutional neural network and multi-objective enhanced Capuchin Search Algorithm. J. Parall. Distrib. Comput. **175**, 1–21 (2023)
28. Seyfollahi, A., Ghaffari, A.: A review of intrusion detection systems in RPL routing protocol based on machine learning for internet of things applications. Wirel. Commun. Mob. Comput. **2021**(1), 8414503 (2021)
29. Ghanbarzadeh, R., Hosseinalipour, A., Ghaffari, A.: A novel network intrusion detection method based on metaheuristic optimisation algorithms. J. Ambient. Intell. Humaniz. Comput. **14**(6), 7575–7592 (2023)
30. Mohammadi, R., Ghaffari, A.: Optimizing reliability through network coding in wireless multimedia sensor networks. Indian J. Sci. Technol. **83**, 841–884 (2015)
31. Arasteh, B., Abdi, M., Bouyer, A.: Program source code comprehension by module clustering using combination of discretized gray wolf and genetic algorithms. Adv. Eng. Softw. **173**, 103252 (2022)
32. Arasteh, B.: Clustered design-model generation from a program source code using chaos-based metaheuristic algorithms. Neural Comput. Appl. **35**(4), 3283–3305 (2023)
33. Arasteh, B.: Software fault-prediction using combination of neural network and Naive Bayes algorithm. J. Netw. Technol. **9**(3), 95 (2018)
34. A. Pakmehr, A. Aßmuth, C. P. Neumann, and G. Pirkl, Security challenges for cloud or fog computing-based AI applications. arXiv preprint arXiv:231.20230.19459
35. Lohachab, A., Karambir, B.: Critical analysis of DDoS: an emerging security threat over IoT networks. J. Commun. Inform. Netw. **3**, 57–78 (2018)
36. Sicari, S., Rizzardi, A., Miorandi, D., Coen-Porisini, A.: REATO: REActing TO denial of service attacks in the internet of things. Comput. Netw. **137**, 37–48 (2018)
37. Pakmehr, A., Gholipour, M., Zeinali, E.: ETFC: energy-efficient and deadline-aware task scheduling in fog computing. Sustain. Comput. **87**, 100988 (2024)
38. Ali, B.H., Jalal, A.A., Al-Obaydy, W.N.I.: Data loss prevention by using MRSH-v2 algorithm. Int. J. Electr. Comput. Eng **10**, 3615–3622 (2020)
39. Osborne, C.: The average DDoS attack cost for businesses rises to over $2.5 million. Web Document **21**, 2018 (2017)
40. K. Wehbi, L. Hong, T. Al-salah, and A. A. Bhutta, A survey on machine learning based detection on DDoS attacks for IoT systems. In: 2019 SoutheastCon, 2019, pp. 1–6: IEEE.
41. A. Shirmarz, A. Ghaffari, R. Mohammadi, and S. Akleylek, "DDOS attack detection accuracy improvement in software defined network (SDN) using ensemble classification. In 2021 International Conference on Information Security and Cryptology (ISCTURKEY), 2021, pp. 111–115: IEEE.
42. Garba, U.H., Toosi, A.N., Pasha, M.F., Khan, S.: SDN-based detection and mitigation of DDoS attacks on smart homes. Comput. Commun. **221**, 29–41 (2024)
43. Vishwakarma, R., Jain, A.K.: A survey of DDoS attacking techniques and defence mechanisms in the IoT network. Telecommun. Syst. **73**(1), 3–25 (2020)
44. P. B. Pajila and E. G. Julie, Detection of DDoS attack using SDN in IoT: a survey. In: Intelligent Communication Technologies and Virtual Mobile Networks: ICICV 2019, 2020, pp. 438–452: Springer.
45. Aamir, M., Zaidi, M.A.: A survey on DDoS attack and defense strategies: from traditional schemes to current techniques. Interdiscip. Inf. Sci. **19**(2), 173–200 (2013)
46. Yu, S., Zhou, W., Doss, R., Jia, W.: Traceback of DDoS attacks using entropy variations. IEEE Trans. Parall. Distrib. Syst. **22**(3), 412–425 (2010)
47. Liu, Y., Cukic, B., Gururajan, S.: Validating neural network-based online adaptive systems: a case study. Software Qual. J. **15**(3), 309–326 (2007)
48. P. Kamboj, M. C. Trivedi, V. K. Yadav, and V. K. Singh, Detection techniques of DDoS attacks: a survey. In: 2017 4th IEEE Uttar Pradesh section international conference on electrical, computer and electronics (UPCON), 2017, pp. 675–679: IEEE
49. A. Srivastava, B. B. Gupta, A. Tyagi, A. Sharma, and A. Mishra A recent survey on DDoS attacks and defense mechanisms. In: International Conference on Parallel Distributed Computing Technologies and Applications, 2011, pp. 570–580: Springer.
50. Sood, I., Sharma, V.: Computational intelligent techniques to detect ddos attacks: a survey. J. Cybersecur. **3**(2), 89 (2021)
51. Alkasassbeh, M., Al-Naymat, G., Hassanat, A.B., Almseidin, M.: Detecting distributed denial of service attacks using data mining techniques. Int. J. Adv. Comput. Sci. Appl. **7**(1), 1 (2016)
52. Mahjabin, T., Xiao, Y., Sun, G., Jiang, W.: A survey of distributed denial-of-service attack, prevention, and mitigation techniques. Int. J. Distrib. Sens. Netw. **13**(12), 1550147717741463 (2017)
53. Gaurav, A., Gupta, B.B., Alhalabi, W., Visvizi, A., Asiri, Y.: A comprehensive survey on DDoS attacks on various intelligent systems and it's defense techniques. Int. J. Intell. Syst. **37**(12), 11407–11431 (2022)
54. Sattar, I., Shahid, M., Abbas, Y.: A review of techniques to detect and prevent distributed denial of service (DDoS) attack in cloud computing environment. Int. J. Comput. Appl. **115**(8), 23–27 (2015)
55. Y. Kim, W. C. Lau, M. C. Chuah, and H. J. Chao, PacketScore: Statistics-based overload control against distributed denial-of-service attacks. In: IEEE INFOCOM 2004, 2004, vol. 4, pp. 2594–2604: IEEE.
56. Jasim, A.D.: A survey of intrusion detection using deep learning in internet of things. Iraqi J. For Comput. Sci. Math. **3**(1), 83–93 (2022)

57. Ding, Y., Zhang, W., Zhou, X., Liao, Q., Luo, Q., Ni, L.M.: FraudTrip: taxi fraudulent trip detection from corresponding trajectories. IEEE Internet Things J. **8**(16), 12505–12517 (2020)
58. Almaraz-Rivera, J.G., Perez-Diaz, J.A., Cantoral-Ceballos, J.A.: Transport and application layer DDoS attacks detection to IoT devices by using machine learning and deep learning models. Sensors **22**(9), 3367 (2022)
59. V. Harikrishnan, H. Sanket, K. Sahazeer, S. Vinay, and P. B. Honnavalli, Mitigation of DDoS attacks using honeypot and firewall. In: Proceedings of Data Analytics and Management: ICDAM 2021, Volume 2, 2022, pp. 625–635: Springer.
60. Jaafar, G.A., Abdullah, S.M., Ismail, S.: Review of recent detection methods for HTTP DDoS attack. J. Comput. Netw. Commun. **2019**(1), 1283472 (2019)
61. Bouabdellah, M., Kaabouch, N., El Bouanani, F., Ben-Azza, H.: Network layer attacks and countermeasures in cognitive radio networks: a survey. J. Inform. Secur. Appl. **38**, 40–49 (2018)
62. Li, W., Tug, S., Meng, W., Wang, Y.: Designing collaborative blockchained signature-based intrusion detection in IoT environments. Futur. Gener. Comput. Syst. **96**, 481–489 (2019)
63. S. Tug, W. Meng, and Y. Wang, "CBSigIDS: towards collaborative blockchained signature-based intrusion detection In: 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2018, pp. 1228–1235: IEEE.
64. Salam, M.A.: Intelligent system for IoT botnet detection using SVM and PSO optimization. J. Intell. Syst. Internet Things **3**(2), 68–84 (2021)
65. M. M. Azmi and F. D. S. Sumadi, "Low-rate attack detection on SD-IoT using SVM combined with feature importance logistic regression coefficient. In: Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control, 2022.
66. Paradise, P., Prabowo, W.A., Rijanandi, T.: Analysis of distributed denial of service attacks using support vector machine and fuzzy Tsukamoto. J Media Inform Budidarma **7**(1), 66–73 (2023)
67. Al-Shorman, A., Faris, H., Aljarah, I.: Unsupervised intelligent system based on one class support vector machine and Grey Wolf optimization for IoT botnet detection. J Ambient Intell Hum Comput **11**(7), 2809–2825 (2020)
68. Suprayogi, C., Marwan, M.A.: Classification of network traffic data Mirai malware attacks on internet of things devices using the k-nearest neighbor method. Int. Res. J. Adv. Eng. Sci. **7**(4), 39–43 (2022)
69. S. Salaria, S. Arora, N. Goyal, P. Goyal, and S. Sharma, Implementation and Analysis of an Improved PCA technique for DDoS Detection." In: *2020 IEEE 5th International Conference on Computing Communication and Automation (ICCCA)*, 2020, pp. 280–285: IEEE.
70. Jasim, M.N., Gaata, M.T.: K-Means clustering-based semi-supervised for DDoS attacks classification. Bull. Electr. Eng. Inform. **11**(6), 3570–3576 (2022)
71. Gu, Y., Li, K., Guo, Z., Wang, Y.: Semi-supervised K-means DDoS detection method using hybrid feature selection algorithm. IEEE Access **7**, 64351–64365 (2019)
72. R. T. Wiyono and N. D. W. Cahyani, Performance analysis of decision tree c4. 5 as a classification technique to conduct network forensics for botnet activities in internet of things," In: *2020 International Conference on Data Science and Its Applications* (*ICoDSA*), 2020, pp. 1–5: IEEE.
73. Padmashree, A., Krishnamoorthi, M.: Decision tree with pearson correlation-based recursive feature elimination model for attack detection in IoT environment. Inform. Technol. Control **51**(4), 771–785 (2022)
74. G. Lucky, F. Jjunju, and A. Marshall, A lightweight decision-tree algorithm for detecting DDoS flooding attacks. In: *2020 IEEE 20th international conference on software quality, reliability and security companion (QRS-C)*, 2020, pp. 382–389: IEEE.
75. Yu, J., Kang, H., Park, D., Bang, H.-C., Kang, D.W.: An in-depth analysis on traffic flooding attacks detection and system using data mining techniques. J. Syst. Architect. **59**(10), 1005–1012 (2013)
76. Widiyasono, N., Giriantari, I.D., Sudarma, M., Linawati, L.: Detection of Mirai malware attacks in IoT environments using random forest algorithms. TEM J. **10**(3), 1209–1219 (2021)
77. Stiawan, D., Idris, M.Y.B., Defit, S., Triana, Y.S., Budiarto, R.: Improvement of attack detection performance on the internet of things with PSO-search and random forest. J. Comput. Sci. **64**, 101833 (2022)
78. A. Gupta and A. Kumar, Standard scaling and PCA-based logistic regression model for classifying and detecting DDoS attack. 2023.
79. Abbasi, F., Naderan, M., Alavi, S.E.: Intrusion detection in IoT with logistic regression and artificial neural network: Further investigations on n-baIoT dataset devices. J. Comput. Secur. **8**(2), 27–42 (2021)
80. Jewani, M.V.K., Ajmire, P.E., Brijwani, M.G.N., Ramola, M.A.: Machine learning classification and prediction techniques to detect DDOS attack. IEEE Access **10**(2022), 21443–21454 (2022)
81. S. Sambangi and L. Gondi, A machine learning approach for ddos (distributed denial of service) attack detection using multiple linear regression. In: *Proceedings*, 2020, vol. 63, no. 1, p. 51: MDPI.
82. Vishwakarma, M., Kesswani, N.: A new two-phase intrusion detection system with Naïve Bayes machine learning for data classification and elliptic envelop method for anomaly detection. Decis. Anal. J. **7**, 100233 (2023)
83. Mehmood, A., Mukherjee, M., Ahmed, S.H., Song, H., Malik, K.M.: NBC-MAIDS: Naïve Bayesian classification technique in multi-agent system-enriched IDS for securing IoT against DDoS attacks. J. Supercomput. **74**, 5156–5170 (2018)
84. Wang, Q., Hu, J., Wu, Y., Zhao, Y.: Output synchronization of wide-area heterogeneous multi-agent systems over intermittent clustered networks. Inf. Sci. **619**, 263–275 (2023)
85. Hnamte, V., Balram, G.: Implementation of Naive Bayes classifier for reducing DDoS attacks in IoT networks. J. Algebr. Stat. **13**(2), 2749–2757 (2022)
86. Dhaliwal, S.S., Nahid, A.-A., Abbas, R.: Effective intrusion detection system using XGBoost. Information **9**(7), 149 (2018)
87. J. A. Faysal et al. XGB-RF: A hybrid machine learning approach for IoT intrusion detection. In: *Telecom*, 2022, vol. 3, no. 1, pp. 52–69: MDPI.
88. S. Khan, Lightweight deep learning framework to detect botnets in iot sensor networks by using hybrid self-organizing map. 2020.
89. Almiani, M., AbuGhazleh, A., Jararweh, Y., Razaque, A.: DDoS detection in 5G-enabled IoT networks using deep Kalman backpropagation neural network. Int. J. Mach. Learn. Cybern. **12**(11), 3337–3349 (2021)
90. Almotiri, J.: DDoS intrusion detection model for IoT networks using backpropagation neural network. Int. J. Adv. Comput. Sci. Appl. **13**(6), 6 (2022)
91. A. R. Shaaban, E. Abd-Elwanis, and M. Hussein, DDoS attack detection and classification via Convolutional Neural Network (CNN). In: *2019 Ninth International Conference on Intelligent*

Computing and Information Systems (ICICIS), 2019, pp. 233–238: IEEE.
92. Wang, J., Liu, Y., Feng, H.: IFACNN: efficient DDoS attack detection based on improved firefly algorithm to optimize convolutional neural networks. Math. Biosci. Eng. **19**(2), 1280–1303 (2022)
93. Nie, L., et al.: Intrusion detection for secure social internet of things based on collaborative edge computing: a generative adversarial network-based approach. IEEE Trans. Comput. Soc. Syst. **9**(1), 134–145 (2021)
94. Shroff, J., Walambe, R., Singh, S.K., Kotecha, K.: "Enhanced security against volumetric DDoS attacks using adversarial machine learning. Wirel. Commun. Mobile Comput. **20**, 22 (2022)
95. Y. Li and Y. Lu, "LSTM-BA: DDoS detection approach combining LSTM and Bayes," in *2019 seventh international conference on advanced cloud and big data (CBD)*, 2019, pp. 180–185: IEEE.
96. Alamer, L., Shadadi, E.: DDoS attack detection using long-short term memory with bacterial colony optimization on IoT environment. J. Internet Serv. Inform. Secur. **13**(1), 44–53 (2023)
97. Qamar, R., Zardari, B., Arain, A., Khoso, F., Jokhio, A.: Detecting distributed denial of service attacks using recurrent neural network. Psychology **2022**, 1 (2022)
98. Wang, M., Lu, Y., Qin, J.: A dynamic MLP-based DDoS attack detection method using feature selection and feedback. Comput. Secur. **88**, 101645 (2020)
99. Manimurugan, S., Al-Mutairi, S., Aborokbah, M.M., Chilamkurti, N., Ganesan, S., Patan, R.: Effective attack detection in internet of medical things smart environment using a deep belief neural network. IEEE Access **8**, 77396–77404 (2020)
100. Hajtmanek, R., Kontšek, M., Smieško, J., Uramová, J.: One-parameter statistical methods to recognize DDoS attacks. Symmetry **14**(11), 2388 (2022)
101. T. Andrysiak and Ł. Saganowski, Ddos attacks detection by means of statistical models. In *Proceedings of the 9th International Conference on Computer Recognition Systems CORES 2015*, 2016, pp. 797–806: Springer.
102. Katib, I., Ragab, M.: Blockchain-assisted hybrid harris hawks optimization based deep DDoS attack detection in the IoT environment. Mathematics **11**(8), 1887 (2023)
103. Ibrahim, R.F., Al-Haija, Q.A., Ahmad, A.: "DDoS attack prevention for internet of thing devices using ethereum blockchain technology. Sensors **22**(18), 6806 (2022)
104. Zhou, L., Guo, H., Deng, G.: A fog computing based approach to DDoS mitigation in IIoT systems. Comput. Secur. **85**, 51–62 (2019)
105. Hassan, K.F., Manaa, M.E.: Detection and mitigation of DDoS attacks in internet of things using a fog computing hybrid approach. Bull. Electr. Eng. Inform. **11**(3), 1604–1613 (2022)
106. A. Gaurav, B. B. Gupta, C.-H. Hsu, S. Yamaguchi, and K. T. Chui, Fog layer-based DDoS attack detection approach for internet-of-things (IoTs) devices. In *2021 IEEE international conference on consumer electronics (ICCE)*, 2021, pp. 1–5: IEEE.
107. M. E. Ahmed and H. Kim, DDoS attack mitigation in Internet of Things using software defined networking. In: *2017 IEEE third international conference on big data computing service and applications (BigDataService)*, 2017, pp. 271–276: IEEE.
108. Bhayo, J., Jafaq, R., Ahmed, A., Hameed, S., Shah, S.A.: A time-efficient approach toward DDoS attack detection in IoT network using SDN. IEEE Internet Things J. **9**(5), 3612–3630 (2021)
109. N. Fadhel, H. F Atlam, and E. Mwangi, Malicious activity detection using smart contracts in IoT. 2021.
110. Ma, J., Hu, J.: Safe consensus control of cooperative-competitive multi-agent systems via differential privacy. Kybernetika **58**(3), 426–439 (2022)
111. M. F. Saiyed and I. Al-Anbagi, Deep ensemble learning with pruning for DDoS attack detection in IoT networks. In: *IEEE Transactions on Machine Learning in Communications and Networking,* 2024.
112. Ghaffari, A., Jelodari, N., Pouralish, S., Derakhshanfard, N., Arasteh, B.: "Securing internet of things using machine and deep learning methods: a survey. Clust. Comput. **5**, 1–25 (2024)
113. Dai, X., et al.: Task co-offloading for D2D-assisted mobile edge computing in industrial internet of things. IEEE Trans. Industr. Inf. **19**(1), 480–490 (2022)

Amir Pakmehr is a Ph.D. student in Computer Engineering, specializing in the Internet of Things, Fog Computing, and Optimization Algorithms. His research primarily focuses on enhancing the scalability and energy efficiency of cloud and fog computing environments. He has authored numerous papers that significantly advance these technologies, contributing to more scalable and energy-efficient solutions.

Andreas Aßmuth received his diploma in Electrical Engineering and Information Technology and the degree "Doctor of Engineering" from Universität der Bundeswehr München, Germany. He became Professor of Computer Networks and Mathematics at Ostbayerische Technische Hochschule (OTH) Amberg-Weiden, Amberg, Germany, in 2011. His research areas are Information Security, Applied Cryptography and Ethical Hacking. In addition to the topics in the denomination of his professorship, he represents his research topics in teaching as well. He is an IEEE Member and an IARIA Fellow.

Negar Taheri received the B.Sc. degree in software engineering from UCASJ (Applied science of Jahad) University, Tabriz, Iran, and the M.Sc. degree in software engineering from Science and Research Branch, Islamic Azad University, Ardabil, Iran, respectively in 2014, and 2018. She is currently a Ph.D. student in Computer Engineering at Islamic Azad University, Tabriz Branch. Her research interests include Internet of Things, artificial intelligence, and wireless sensor networks.

Ali Ghaffari received his B.Sc., M.Sc. and Ph.D. degrees in computer engineering from the University of Tehran and IAU (Islamic Azad University), Tehran, Iran in 1994, 2002 and 2011 respectively. He has served as a reviewer for some high-ranked journal such as IEEE transaction on mobile computing, IEEE/ACM Transactions on Networking, IEEE Transactions on Network and Service Management, Applied Soft Computing, Ad Hoc networks, Future Generation Computer System (FGCS), Journal of Ambient Intelligent and Humanized Computing (AIHC) and computer networks. He has been featured among the World's Top 2% Scientists List in computer science, according to a conducted study by US-based Stanford University in 2020, and 2021 and Top 1% Scientists List in computer science, according to Clarivate analytics in 2022 and 2023. His research interests are mainly in the field of software defined network (SDN), Wireless Sensor Networks (WSNs), Mobile Ad Hoc Networks (MANETs), Vehicular Ad Hoc Networks (VANETs), networks security and Quality of Service (QoS). He has published more than 200 international conference and reviewed journal papers.