The Journal of Supercomputing (2024) 80:9986–10043
https://doi.org/10.1007/s11227-023-05843-7

Iot traffic-based DDoS attacks detection mechanisms: A comprehensive review

Praveen Shukla[1] · C. Rama Krishna[1] · Nilesh Vishwasrao Patil[2]

Accepted: 26 November 2023 / Published online: 19 December 2023

Abstract

The Internet of Things (IoT) has emerged as an inevitable part of human life, that includes online learning, smart homes, smart cars, smart grids, smart cities, agriculture, and e-healthcare. It allows us to operate them 24/7 from anywhere. These smart IoT devices streamline our daily lives by automating everything around us. Several security issues have arisen with the continuous growth of non-secure IoT devices. Distributed Denial of Service (DDoS) attack is one of the most prominent security threats to Internet-based services and IoT platforms. It has the potential to break down the victim's server or network by transferring an immense amount of irrelevant traffic from the pool of compromised IoT devices. In this article, we present: (i) A comprehensive cyberattacks taxonomy for IoT platforms, (ii) Systematically demonstrate IoT technology: evolution, applications, and challenges, (iv) Systematic review of existing machine learning (ML) and deep learning (DL)-based detection approaches for large-scale IoT traffic-based DDoS attacks, (v) Characterize publicly available IoT-traffic-specific datasets, and (vi) Discuss various open research issues with possible solutions for detecting IoT traffic-based DDoS attacks, including future directions.

Keywords Internet of Things (IoT) · IoT platforms · Distributed denial of service (DDoS) attacks · Machine learning · Deep learning · Cyberattacks taxonomy.

✉ Nilesh Vishwasrao Patil
nilesh.cse18@nitttrchd.ac.in

[1] Department of Computer Science & Engineering, National Institute of Technical Teachers Training & Research, Chandigarh, Panjab University, Chandigarh, India

[2] Department of Computer Engineering, Government Polytechnic, Chhatrapati Sambhajinagar (Aurangabad), Maharashtra, India

1 Introduction

In this modern era, IoT is a rapidly growing technology that connects everything with the Internet to exchange data without human intervention [1]. There are billions of interconnected devices equipped with sensors and software that can collect or transfer information with each other through public networks. Users can easily access these devices 24/7 from anywhere. IoT devices have been gaining popularity since the last decade in society and industries due to their ease of use, affordability, compact size, and low power consumption. Further, as per a recent report, the market of IoT devices is expected to grow up to 1.6 trillion US dollars by 2025 [2].

IoT applications are widely spread across every industry and sector, including smart homes, offices, smart cities, transportation, agriculture, healthcare, education, defense, and so on. It has brought significant advantages and smartness to our lives, society, and enterprises. Despite that, this technology is not mature enough to provide assured security in services. Therefore, security is one of the most significant concerns. A recent report claims that, there will be twenty-nine billion IoT devices connected to public networks by 2030 [3], as depicted in Fig. 1. Further, various IoT devices containing valuable information of users [4, 5]. For instance, they store personal data about the customer, such as their location, contact information, health details, etc., that can be compromised.

However, the day-by-day increase in non-secure IoT devices brings various security issues due to the limited resources (memory, processor, power, and bandwidth) and lack of security features. Therefore, cybercriminals accumulate more opportunities to acquire access to these devices, compromise them, and then execute large-scale DDoS attacks with these devices. Several detection solutions have been provided in the literature to defend against IoT traffic-based-DDoS attacks for protecting the IoT environment. Therefore, examining machine learning and deep learning-based DDoS attack detection approaches is a super-heated topic among academicians and researchers.

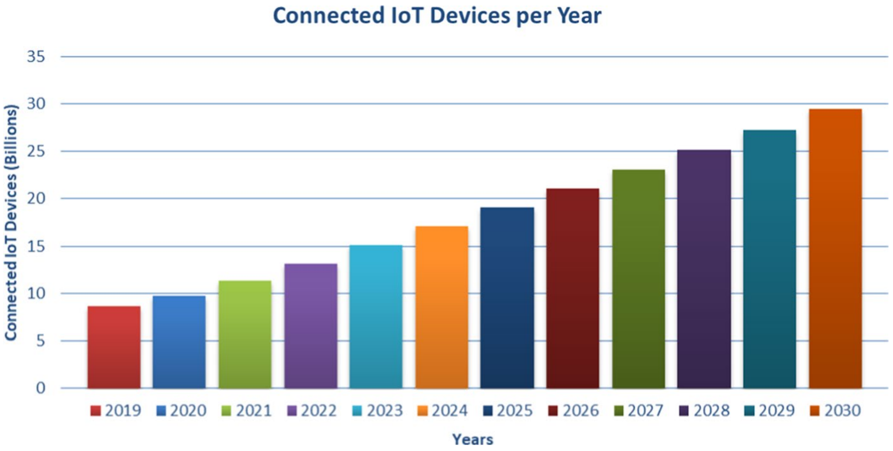

Fig. 1 Year-wise IoT devices connected to public networks [3]

1.1 IoT platform

The extensive IoT network consists of millions of interconnected physical objects, such as sensors, computers, machines, digital devices, etc. In this, diverse smart gadgets with distinct functionalities communicate seamlessly with each other. Their primary purpose is to collect, analyze, and process information to make decisions without human assistance. Hence, this contributes to automation and improved decision-making based on the data it gathers and processes. This interconnected system generates an intelligent ecosystem where devices work together, enhancing efficiency and improving customer services. Eventually, it simplifies everyday processes and makes our lives more convenient.

1.1.1 Evolution of IoT

IoT technology has been evolved from one or two devices to the use of IoT devices in every household, and the chronological development of IoT technology is illustrated in Figure ??. It is believed that the concept of the IoT was born after 1999 when Kevin Ashton introduced the term IoT during his presentation at Proctor and Gamble, MIT [6]. However, before 1999 several attempts have been made to design intelligent devices. For example, in 1982, researchers at Carnegie Mellon University connected a vending machine to the Internet to test cold soda remotely [7]. Moreover, a smart toaster, invented by John Romkey in 1990, was the first IoT device that operated using the Internet [8]. In the 1990 s, IoT technology witnessed many developments, ranging from Steve Mann's wearable webcam to the US government's long-term GPS satellite program [9].

LG brought the world's first Wi-Fi-enabled smart refrigerator in 2000 [10]. The first smartwatch was launched in 2004 as part of this development journey. In the same year, US Department of Defense successfully deployed the RFID systems on a large scale [7]. Apple Inc. released iPhone and wearable Fitbit in 2007. After that, the first international conference on IoT was held in Switzerland in 2008, attended by 250 researchers from 23 different countries [9]. It can be considered a significant event for the growth and popularity of IoT.

IoT reached a new dimension in 2009 when Google started testing self-driving cars. Further, 2011 was another landmark year for IoT as Gartner added IoT to their Hype cycle of emerging technologies [10]. In 2013 Google smart glasses, followed by Amazon Echo in 2014. It has been accepted as a revolutionary step in IoT and wearable technology. These inventions in the IoT technology open a way to enter in the smart home market [9]. In 2015, Elon Mask released the Autopilot feature in smart cars, which allows drivers to focus on other things while driving [7]. Despite groundbreaking technological advancements in IoT environment over the past few years, in 2016, the first major IoT malware attack was carried out on Dyn's server using the Mirai botnet [10].

In 2018, IoT technology was integrated with smart-healthcare applications to monitor patients' health remotely [8]. However, this growth in IoT devices has also increased IoT-based cyberattacks. More than 1.5 billion attacks were executed on IoT devices in the first half of 2021 [11]. Therefore, securing IoT devices from different types of cyberattacks has become a topmost priority for manufacturers and customers (Fig. 2).

1.1.2 Applications of IoT

IoT technology offers a wide range of technical solutions for every aspect of daily life. Therefore, it has dominated every sector. In Fig. 3, we systematically present the most popular and fast-growing applications related to IoT technology.

For example, the conventional healthcare system has become automated with the integration of IoT technology. During the COVID-19 pandemic, there has been a rise in the demand for IoT-based remote monitoring systems. Integrating IoT into the healthcare domain, we can access modernized devices, such as Internet-connected equipment, wearable fitness gadgets, tracking devices, etc., which help to add smartness to the healthcare domain. The IoT-based device empowers patients and physicians to operate pocket-friendly solutions [12, 13]. Further, in the automobile sector, IoT technology has played a vital role in connected vehicles and reshaped the perception of cars among people. Smart infrastructure and fully automatic connected vehicles together will significantly change the driving experience [14]. Several IoT applications generate global interest, but smart homes and cities are the most prevalent. Home automation, smarter traffic signaling, waste management solutions, e-commerce, monitoring air quality, digital entertainment, and distribution system of water, and energy are some instances of IoT applications utilized to address fundamental problems of society like air/noise pollution, traffic jams, inadequate energy, and water supplies, among many others [15]. Further, IoT technology has contributed significantly to the development of Smart Farming and Smart Grid technologies, which have transformed conventional farming practices and energy management systems [16, 17]. For example with the help of sensors, one can monitor the harvest field from anywhere and utilize resources (water, electricity) more efficiently.

1.2 Challenges

IoT technology is still in its infancy with respect to security and faces several research challenges. They are systematically presented in Fig. 4. In addition to their small and lightweight design, IoT devices also have limited processing and storage capacities, resulting in several manufacturers introducing IoT devices with multiple security loopholes. Further, standardized protocols and technologies required to design and implement these devices may be compromised due to less processing capabilities. Therefore, cybercriminals exploit vulnerabilities of numerous non-secure IoT devices and compromise them to form a bot army for executing large-scale attacks [18, 19].

In the addition, several renowned high-tech companies and government organizations across the globe suffered from large-scale DDoS attacks. Therefore, numerous security and privacy breaches in the current IoT system have motivated research

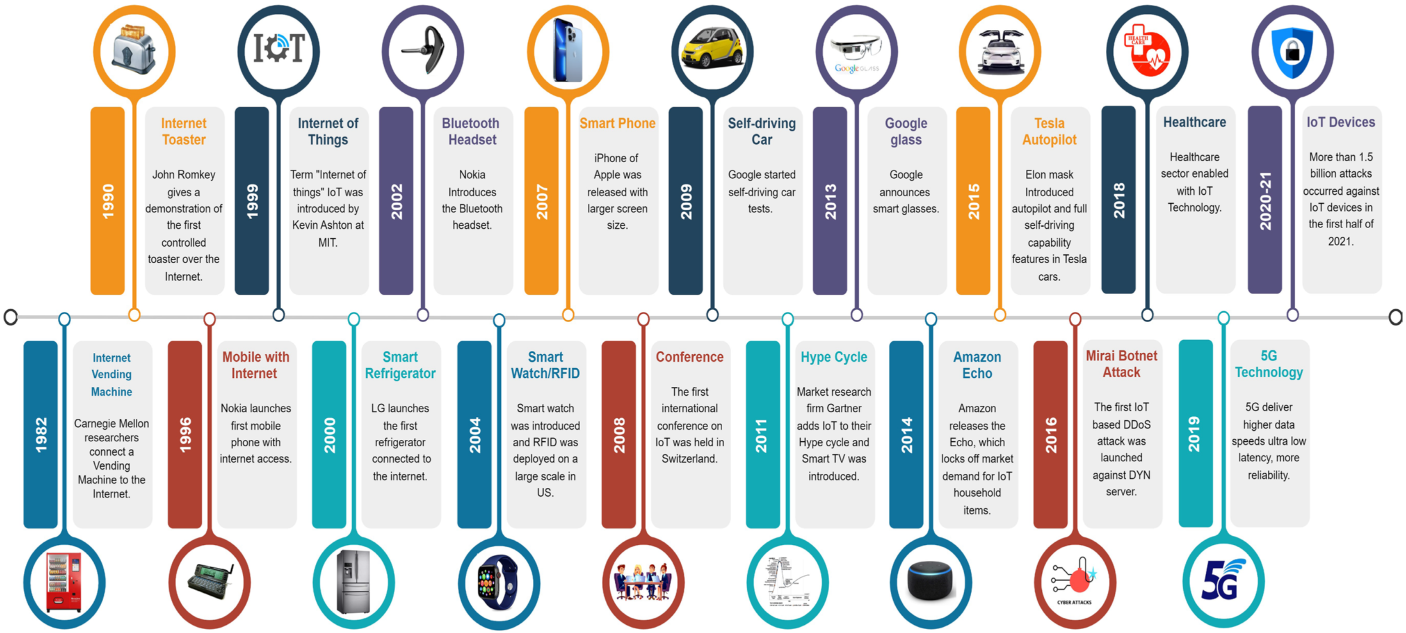
1982
Internet Vending Machine
Carnegie Mellon researchers connect a Vending Machine to the Internet.
1990
Internet Toaster
John Romkey gives a demonstration of the first controlled toaster over the Internet.
1996
Mobile with Internet
Nokia launches first mobile phone with internet access.
1999
Internet of Things
Term "Internet of things" IoT was introduced by Kevin Ashton at MIT.
2000
Smart Refrigerator
LG launches the first refrigerator connected to the internet.
2002
Bluetooth Headset
Nokia Introduces the Bluetooth headset.
2004
Smart Watch/RFID
Smart watch was introduced and RFID was deployed on a large scale in US.
2007
Smart Phone
iPhone of Apple was released with larger screen size.
2008
Conference
The first international conference on IoT was held in Switzerland.
2009
Self-driving Car
Google started self-driving car tests.
2011
Hype Cycle
Market research firm Gartner adds IoT to their Hype cycle and Smart TV was introduced.
2013
Google glass
Google announces smart glasses.
2014
Amazon Echo
Amazon releases the Echo, which locks off market demand for IoT household items.
2015
Tesla Autopilot
Elon mask Introduced autopilot and full self-driving capability features in Tesla cars.
2016
Mirai Botnet Attack
The first IoT based DDoS attack was launched against DYN server.
2018
Healthcare
Healthcare sector enabled with IoT Technology.
2019
5G Technology
5G deliver higher data speeds ultra low latency, more reliability.
2020-21
IoT Devices
More than 1.5 billion attacks occurred against IoT devices in the first half of 2021.

Fig. 2 A comprehensive timeline of major developments' in IoT technology

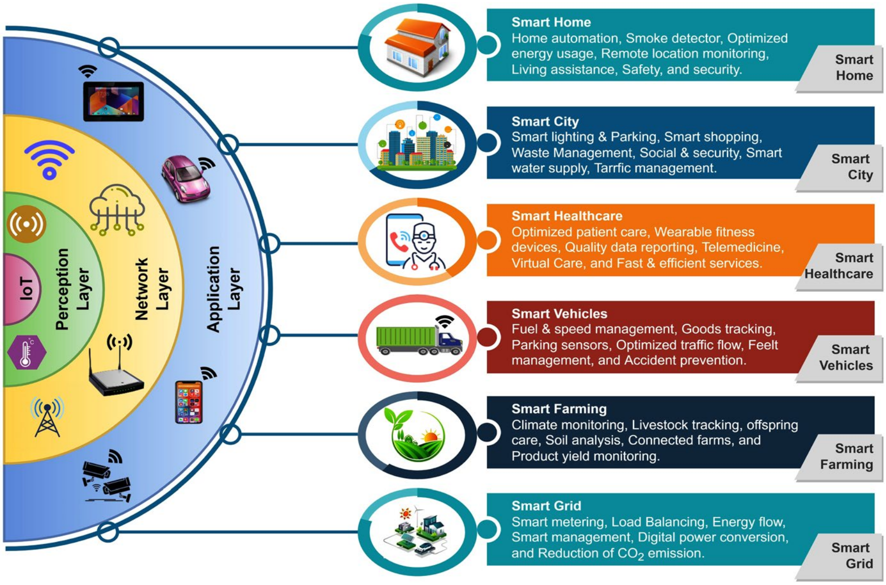
IoT
Perception Layer
Network Layer
Application Layer
Smart Home
Home automation, Smoke detector, Optimized energy usage, Remote location monitoring, Living assistance, Safety, and security.
Smart Home
Smart City
Smart lighting & Parking, Smart shopping, Waste Management, Social & security, Smart water supply, Tarrfic management.
Smart City
Smart Healthcare
Optimized patient care, Wearable fitness devices, Quality data reporting, Telemedicine, Virtual Care, and Fast & efficient services.
Smart Healthcare
Smart Vehicles
Fuel & speed management, Goods tracking, Parking sensors, Optimized traffic flow, Feelt management, and Accident prevention.
Smart Vehicles
Smart Farming
Climate monitoring, Livestock tracking, offspring care, Soil analysis, Connected farms, and Product yield monitoring.
Smart Farming
Smart Grid
Smart metering, Load Balancing, Energy flow, Smart management, Digital power conversion, and Reduction of CO2 emission.
Smart Grid

Fig. 3 A graphical representation of IoT applications using a layered architecture

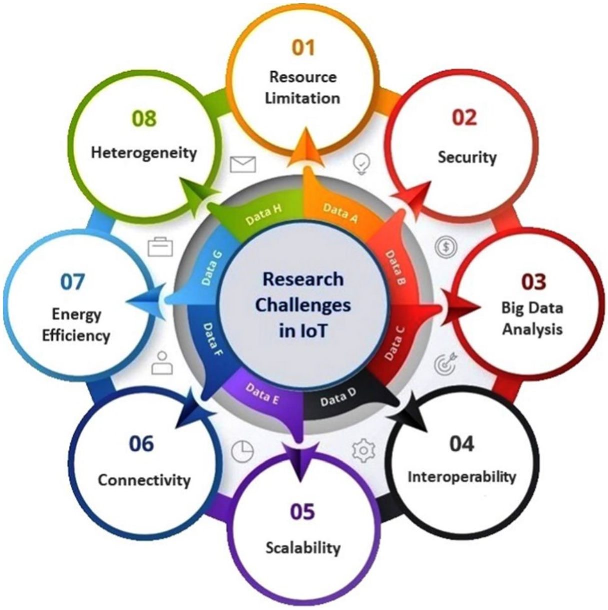

Fig. 4 Research challenges in IoT technology

communities to develop a comprehensive solution for enhancing the security of IoT-enabled industries/sectors.

One of the most prominent examples of the heterogeneity issue in the IoT environment is that it comprises a vast array of distributed devices, such as sensors, actuators, and other gadgets [20].

Interoperability refers to the ability of different systems or devices "speak the same language" with respect to encoding and protocols. It creates a common path to share data and perform tasks together to achieve the same goal. However, several industries employ different communication technologies, protocols, and components for designing IoT applications that generate a wide range of data specific to their business field. Due to this heterogeneous environment, IoT-based systems encounter difficulties while interacting with each other.

Data management is an exceptionally challenging task due to the heterogeneous nature of IoT devices. Further, they generate lots of data for storing and processing. Traditional database management systems and software techniques have failed to handle Big Data [37]. As per the current scenario, numerous IoT-based systems use traditional cloud architectures to send and receive the large volumes of data generated and consumed by IoT-enabled gadgets. Furthermore, performing highly computational jobs effectively and securely on cloud platforms remains a constant concern [38]. Therefore, systematically analyzing lots of data generated by IoT-based networks is another challenge for IoT systems. One of the emerging fields of Big Data is IoT-based systems, such as virtual assistants (Amazon Alexa, Microsoft's Cortana, and Apple's Siri) that generate massive amounts of data regularly. According to Forbes, there were 35 times as many voice searches in 2016 than in 2008, and 33 million voice-first devices are currently in service [39].

In Table 1, we systematically presented several challenges concerning IoT devices and technology. It includes mobility, standardization, low cost, scalability, connectivity, self-organization, maintenance, up-gradation, energy efficiency, full Internet access, and quality of service. A list of abbreviations/ terminologies used in this study is summarized in Table 2.

1.3 Contributions

The significant contributions of this review article are listed in the following:

1. Comprehensively examine various security issues associated with the IoT environment and proposed a comprehensive cyberattacks taxonomy for IoT platforms, characterizing each class of taxonomy w.r.t. the layered architecture of IoT and traffic flow rate.
2. Systematically present IoT technology w.r.t its evolution, applications, and various challenges.
3. Critically analyze the existing Machine Learning (ML) and Deep Learning (DL)-based detection approaches for large-scale IoT traffic-based DDoS attacks.
4. Characterize various publically available IoT-traffic-specific datasets.

Table 1 Summary of research challenges in IoT system

Authors	Year	Challenges	Description
Zafeiriou et al. [21]	2020	Mobility	IoT-based automobiles (e.g., smart cars) may face mobility challenges
			Building trust is relatively easy and more comfortable in slow-moving than in fast-moving IoT-based applications
Ryan et al. [22]	2017	Standardization	Standardization is to define a set of rules for “how to do” the activities at
Ruchi et al. [23]	2020		Different stages of designing, developing, maintaining, and using the IoT
			Government should provide a standard interface for developing IoT applications to achieve the greatest level of compatibility between devices
Attia et al. [24]	2019	Low cost	Multiple brands and companies are entering the IoT manufacturing market
Ahmad et al. [25]	2021		Due to competition, they widely utilize low-cost sensors and components, which makes the network less secure
Imran et al. [26]	2020	Scalability	As per recent statistical data related to the growth of IoT devices, trillions
Yahya et al. [27]	2021		Of devices are connected to the public network that will require connectivity,
Chithaluru et al. [28]	2023		Maintenance, and power simultaneously. Therefore scalability of IoT devices and networks are a prime concern
Banafa A. [29]	2017	Connectivity	Currently, IoT-based devices and networks are followed a centralized comm-unication approach i.e. client–server model. However, in near future, trillions of devices are connected to the public network and existing centralized communication approach will become a bottleneck
Mishra et al. [30]	2021		
Kephart et al. [31]	2005	Self organization	In IoT systems, self-organization is the ability to respond automatically and proactively to varying conditions by using one or more control loops that dynamically reconfigure the behavior of the system on-demand basis
Chithaluru et al. [28]	2023		However, providing optimal routing techniques and self-organizing protocols for widespread heterogeneous IoT networks is still a challenge in this area
Michael et al. [32]	2015	Maintenance and updates	For manufacturers of IoT products, maintenance of devices and networks is the most significant challenge. Providing regular updates to keep low- cost devices secure and operational for a long time needs additional charges from clients. Otherwise, devices would be left at high risk
Tahsien et al. [33]	2020		
Ahmad et al. [25]	2021		
Ali et al. [34]	2015	Energy efficiency	Due to lightweight, lack of storage and power, devices are encumbering the power consumption problem. The durability of batteries usually determines how efficiently sensors perform their work. GPS applications deplete batteries quickly after enabling it on any device

Table 1 (continued)

Authors	Year	Challenges	Description
Dickson [35]	2020	Internet accessibility	Typically, most IoT devices are always connected to the internet with minimum security, which often opens windows for being persecuted by different types of cyberattacks
Ray B. [36]	2016	Quality of service	Quality of service (QoS) governs network traffic and the resources of an IoT application need to provide reliable services. However, it is difficult to provide reliable services for widely deployed heterogeneous IoT networks
Ruchi et al. [23]	2020		
Chithaluru et al. [28]	2023		

Table 2 List of abbreviations

Acronym	Description	Acronym	Description
ANN	Artificial Neural Network	LDAP	Lightweight Directory Access Protocol
BiLSTM	Bidirectional Long Short-Term Memory	LAND	Local Area Network Denial
CSV	Comma-Separated Values	LR	Logistic Regression
CAGR	Compound Annual Growth Rate	LSTM	Long Short-term Memory
CNN	Convolutional Neural Network	ML	Machine Learning
CFS	Correlation-based Feature Selection	MQTT	Message Queuing Telemetry Transport
DT	Decision Tree	MLP	Multilayer Perceptron
DL	Deep Learning	NB	Naïve Bayes
DNN	Deep Neural Network	NTP	Network Time Protocol
DoS	Denial of Services	Pps	Packets per Second
DDoS	Distributed Denial of Services	PCA	Principal Component Analysis
DNS	Domain Name System	QoS	Quality of Service
GR	Gain Ratio	RF	Random Forest
Gbps	Giga Bits per Second	Relu	Rectified Linear Unit
GPS	Global Positioning System	RNN	Recurrent Neural Network
HTTP	HyperText Transfer Protocol	SNMP	Simple Network Management Protocol
IIoT	Industrial Internet of Things	SSDP	Simple Service Discovery Protocol
IG	Information Gain	SGD	Stochastic Gradient Descent
ICMP	Internet Control Message Protocol	SVM	Support Vector Machine
IoT	Internet of Things	SMOTE	Synthetic Minority Oversampling Technique
IP	Internet Protocol	Tbps	Tera Bits per Second
IDS	Intrusion Detection System	TCP	Transmission Control Protocol
KNN	K-Nearest Neighbours	UDP	User Datagram Protocol

5. Systematically present various research issues with possible solutions for protecting Internet-based services and networks.

1.4 Prior reviews

Several review articles have been published in the literature in the domain of IoT security. We have systematically compared this review article with recently published review articles in Table 3, which distinctly highlights the unique contributions of this work. We compared them with several significant parameters, including IoT attack taxonomy, feature engineering, feature selection, dataset analysis, classes of attacks categorized, evaluation metrics, etc. Numerous existing reviews narrow their focus to either ML-based or DL-based detection approaches, but our examination encompasses both ML and DL-based detection methods. This study delves into diverse security issues within the IoT environment, examining numerous public

Table 3 Summary of prior review articles

Review article	Tahsien et al. 2020 [33]	Ruchi et al. 2020 [23]	Yahya et al. 2021 [27]	Patil et al. 2021 [40]	Mishra et al. 2021 [30]	Ahmad et al. 2021 [25]	Mittal et al. 2022 [41]	This article
Focused on IoT security Domain	✓	✓	✓	✗	✓	✓	✗	✓
IoT attack Taxonomy	✗	✓	✗	✗	✗	✓	✗	✓
ML/DL based Techniques	ML	ML	IDS	-	ML/DL	ML/DL	DL	ML/DL
Feature engineering	✗	✗	✗	✗	✓	✗	✓	✓
Feature Selection	✗	✗	✗	✗	✗	✓	✗	✓
Features Utilized	✗	✗	✗	✗	✗	✗	✗	✓
Datasets analysis	✗	✗	✗	✓	✓	✓	✓	✓
IoT three Layered architecture	✓	✓	✓	✗	✗	✗	✗	✓
DDoS attack Mapping to ATT &CK	✗	✗	✗	✗	✗	✗	✗	✓
Practical Implication	✗	✗	✗	✗	✗	✗	✗	✓
Research Gaps or	✓	✓	✓	✓	✓	✓	✓	✓

Table 3 (continued)

Review article	Tahsien et al. 2020 [33]	Ruchi et al. 2020 [23]	Yahya et al. 2021 [27]	Patil et al. 2021 [40]	Mishra et al. 2021 [30]	Ahmad et al. 2021 [25]	Mittal et al. 2022 [41]	This article
Challenges Future Directions	✗	✗	✓	✓	✗	✓	✓	✓
Classes of Attacks Classified	✗	✗	✗	✗	✗	✗	✓	✓

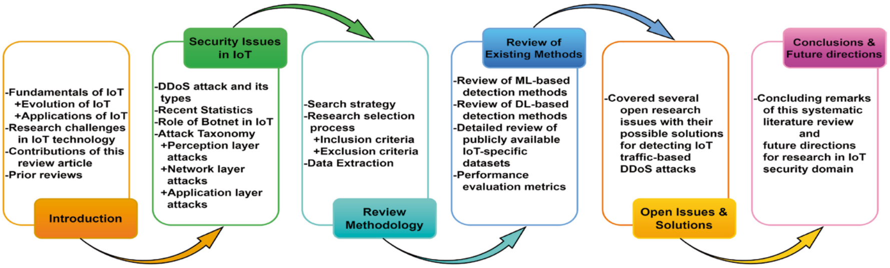
Introduction
-Fundamentals of IoT
+Evolution of IoT
+Applications of IoT
-Research challenges in IoT technology
-Contributions of this review article
-Prior reviews
Security Issues in IoT
-DDoS attack and its types
-Recent Statistics
-Role of Botnet in IoT
-Attack Taxonomy
+Perception layer attacks
+Network layer attacks
+Application layer attacks
Review Methodology
-Search strategy
-Research selection process
+Inclusion criteria
+Exclusion criteria
-Data Extraction
Review of Existing Methods
-Review of ML-based detection methods
-Review of DL-based detection methods
-Detailed review of publicly available IoT-specific datasets
-Performance evaluation metrics
Open Issues & Solutions
-Covered several open research issues with their possible solutions for detecting IoT traffic-based DDoS attacks
Conclusions & Future directions
-Concluding remarks of this systematic literature review and future directions for research in IoT security domain

Fig. 5 A road-map of the systematically conducted literature review

datasets related to IoT traffic that have found widespread utility among researchers. Additionally, we discussed some open research issues to guide researchers in addressing significant security threats such as IoT traffic-based DDoS attacks. Apart from this, it has been observed that several existing review articles failed to address many other parameters as well: (i) Feature engineering or feature selection strategies, (ii) Comprehensive cyberattack taxonomy for IoT platforms, (iii) Classes of attacks classified in the existing literature. It clearly illustrates that our article is unique from the previously published ones.

1.5 Organization of paper

A roadmap of this review article is presented in Fig. 5. In Sect. 2, we present security issues related to the IoT environment and cyberattacks taxonomy with a primary focus on IoT-traffic-based DDoS attacks. Section 3 discusses the systematic review's search strategy, research selection, and data extraction process. Section 4 examines the existing ML, and DL-based detection approaches w.r.t. large-scale IoT traffic-based DDoS attacks and characterization of available datasets utilized to implement cyberattacks detection mechanism. Section 5 illustrates the open issues related to IoT security with feasible solutions. Finally, section 6 concludes this review article with future directions.

2 Security issues in the IoT environment

Protecting IoT devices and networks from different cyberattacks is a critical challenge in front of researchers and organizations. Most of these devices do not have a foolproof security system due to a lack of storage and processing capacity. Therefore, they are susceptible to various security and privacy issues, such as confidentiality, integrity, authentication, access control, etc [42]. Information theft and service interruption are the two most common cybersecurity threats to IoT devices and networks. The IoT incorporates three layers: "the perception layer, the network layer, and the application layer" [43]. Figure 3 depicts a basic three-layer architecture and security threats that adversely impact these layers. Each layer has its strengths and weaknesses that need to be determined. Accordingly, they can ensure their security by preventing various types of attacks [44]. The functions of each layer are given in the following:

1. The perception layer: It is associated with the external world to sense and gather data from its surroundings. Several sensors are used in this layer to measure heat, pH value, light, gas, location, etc [45]. Further, it also catches several functionalities such as humidity, pressure, location, movement, etc. Additionally, actuators operate as controllers to provide mechanical responses based on gathered data. However, this layer is vulnerable to various attacks like jamming, radio interference, eavesdropping, node capturing, malicious code injections, side-channel attacks, etc [46].
2. The network layer: The primary function of this layer is to connect different smart devices, gateways, and servers. Further, it plays an active role in transferring/redirecting the collected data to other IoT network components (computational units) for further processing. Therefore, IoT employs several communication standards and protocols, including 4 G/5 G, 6LoWPAN, ZigBee, Bluetooth, WiFi, WiMAX, etc. [47]. In this layer, local cloud/servers store and process the data, which behaves as an intermediary between the network, and the subsequent layer [48, 49]. However, this layer is highly vulnerable to several attacks like routing attacks, DDoS attacks, ICMP flood, etc.
3. The application layer: The final and farthest layer that provides services to users' requests via mobile devices and web-based software. Numerous innovative applications are available in the application layer to meet the needs of the current trends. They benefit society in many ways through intelligent things, viz. smart cities, smart homes, agriculture, transportation, education, etc [50]. For example, Doctors can use IoT applications to view the health parameters of their patients remotely. However, in this layer, the end-user directly interacts, so there is significant concern about privacy, data theft, etc [51].

Generally, cybercriminals attempt to exploit the open vulnerabilities exist in devices to compromise and gain control of them. It helps to build a massive army of infected devices to launch large-scale attacks. An appropriate security mechanism is required to address these vulnerabilities to prevent cyberattacks. Moreover, conventional security mechanisms are not directly adaptable to IoT technology because of the inherent limitations of their design, such as limited power and a large number of connected things, which boost heterogeneity and scalability issues [52]. In Table 4, we summarizes the various vulnerabilities [23, 30] that exists in the IoT layers/devices [53, 54].

2.1 DDoS attack

A DDoS attack is one of the most significant security-threat to Internet-based applications and IoT environments. It slows down or completely stops the working of the targeted online services (email servers, websites, or anything connected to the Internet) [55]. DDoS attacks not only interrupt services to legitimate users but also lead to considerable financial losses for the targeted industry. For performing large-scale DDoS attacks, attackers gain access to numerous non-secure devices to create an army of compromised devices. Subsequently, each compromised device (bots) transfers attack traffic toward the target system. A typical setup for launching large-scale DDoS attacks is shown in Fig. 6. The distributed nature of the DDoS attack makes it challenging to identify compromised devices and mitigate the impact of the attack immediately. There are three types of DDoS attacks [56, 57]: (i) Volumetric-based attacks, (ii) Application-layer attacks, and (iii) Protocol-based attacks, which are characterized in Table 5. The most common DDoS attacks used for performing attacks are SYN flood attacks, HTTP attacks, UDP attacks, and ICMP attacks.

2.2 Recent statistical information of DDoS attacks

In this section, we present statistical information about recent and large-scale DDoS attack incidents. During the COVID-19 pandemic, there has been a massive growth in the demand for online-based services in every sector. In addition, the commencement of 5 G technologies has accelerated the adoption of IoT technologies across the globe. Therefore, it generates a massive pool of less-secure devices, and it helps to build the large-scale botnet for conducting DDoS attacks [57]. Recent statistical incidents are systematically listed in the following:

1. Due to the Covid-19 situation, each organization moved its services, such as education, healthcare, shopping, etc., to the online mode. Therefore, attackers got opportunities to compromise a large number of non-secure devices and hence, a rise in DDoS attack incidents [57].
2. According to the report [61], in 2021, DDoS attacks decreased by 3% compared to the year 2020. However, the attack volume size and sophistication of attacks grew.
3. As per [61], in the last two years, low-volume DDoS attacks (less than 250 GB) have decreased by approximately 5%. However, the large volume of DDoS attacks increased by 1300%.
4. The significant reason to protect online services can be understood using Fig. 7. It shows that various popular and market-leading organizations have become the victims of large-scale DDoS attacks [57, 58].
5. Several record-breaking, large-scale DDoS attacks have been recorded in the past few years. They are listed as follows: [57–60].

   - In March 2018, the GitHub platform suffered from the third-largest DDoS attack, with the volume size of 1.35 terabits per second (Tbps).
   - In January 2019, the Imperva online service faced one of the largest network and application layer DDoS attacks, such as the SYN DDoS attack with 580 million packets per second (Pps).
   - In Q1-2020, the Amazon platform experienced the second-largest DDoS attack (2 Tbps of data).

Table 4 Summary of the various vulnerabilities in the IoT layers

Vulnerability	Application	Network	Perception	Key points
Insecure Network Connection	✗	✓	✓	The attacker finds it easy to compromise devices if there is no firewall or screening process in place, as they can launch attacks from infected connected devices
Insufficient Authentication /Authorization	✓	✓	✓	Weak passwords are easily breakable by the brute-force method. The default password of most IoT devices are the same across the world, so if the device user doesn't change it, an attacker can easily infect the devices. In the absence of an adequate access control mechanism, an attacker may gain access to a network
Unsafe Network Sservices	✓	✗	✓	Network services that run on the IoT devices in the background, particularly those connected to the Internet, may compromise the integrity/ authenticity of the data and open the possibility of unauthorized control of those devices
Insufficient Transport Encryption	✓	✓	✗	It permits cyber criminals to view information as it passes over local networks or the Internet. IoT network faces considerable risks when you send data as plain text. The most efficient method of preventing data from being intercepted is to encrypt it
Physical Security Threats	✓	✓	✓	Hackers may steal or destroy crucial IT assets, such as servers, secure data centers, or computers on which mission-critical applications run. They can also steal information via USB drives and upload malware onto systems, resulting in huge losses/damages for a business, agency, or institution
Software/ Hardware Flaws	✓	✓	✓	Until a vendor releases a patch, software-related flaws are under the watchful eye of attackers Generally, skilled attackers are capable of finding and exploiting these types of vulnerabilities Due to obsolete firmware, most IoT devices remain unsafe. Hardly, firmware updates are not safe, leaving the device vulnerable
Inadequate Security	✓	✗	✓	Due to their widespread usage and lack of user-friendliness, IoT devices are not as secure as they

Table 4 (continued)

Vulnerability	Application	Network	Perception	Key points
Configuration				could be. Most people don't bother configuring the security of these devices because they're unprofessional, don't have a strong password recovery system, or use unsafe login credentials, making them a more suitable launching pad for cyberattacks

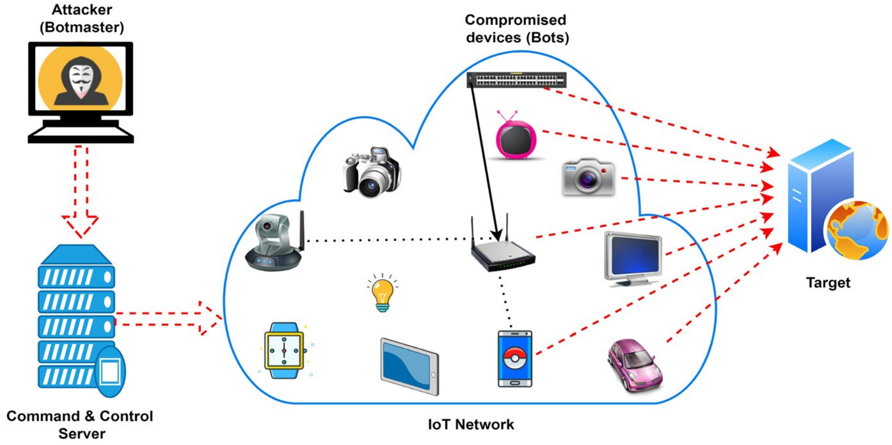

Fig. 6 A typical setup for launching large-scale DDoS attacks using IoT devices [23]

Table 5 Classification of DDoS attacks with mapping to Target techniques

Attack type	Purpose of attack	Magnitude Measured in	Attack sub- Techniques	Examples
Volumetric	To saturate the	Bits	Direct Network Flood,	DNS, NTP Amplified,
Based	bandwidth of	per	Reflection Amplification	TCP flood, UDP flood,
Attack	the target	Second		ICMP flood, CLDAP
Protocol	To consume the	Packets	OS Exhaustion	TCP-SYN flood, ACK flood
Based	server resources,	per	Flood	SSDP flood, Smurf Attack
Attack	firewall, and	Second		RST/FIN flood, LOIC
		load balancers		LAND Attack
Application	To exhaust the	Requests	Application or	HTTP flood, Slowloris
Layer	target application	per	Service Exhaustion,	DNS flood, SIP flood
Attack	resources	Second	System Exploitation	SQL Injection

  - In November 2021, an Azure client experienced the most significant DDoS attack with 3.45 Tbps of throughput and 340 million packets per second (Pps).
  - In 2022, Google successfully handled the most substantial DDoS attacks ever seen, which peaked at approximately 46 million requests per second (rps). However, the recent attack surpassed this, reporting 398 rps and sending 7.5 times more requests than the previous one [62].

6. In 2021, the BFSI (Banking, Financial Services, and Insurance) industries encountered more than 25% of DDoS attacks. Further, the education and telecommunication sectors have experienced a higher percentage of DDoS attacks compared to other sectors [61].
7. As per a recent report [63], the market for providing solutions against different types of DDoS attacks is expected to double to $4.7 billion by 2024. It is representing a compound annual growth rate (CAGR) of 14 percent.

2.3 Role of botnet in IoT traffic-based DDoS attacks

A botnet is a pool of Internet-connected devices compromised by an attacker(s) by installing malicious software or malware (specifically IoT Botnet malware). In this, botmaster (a.k.a attacker) leads the botnet's command-and-control servers for controlling these bots remotely [64]. The security limitations of IoT devices make them vulnerable to compromise, allowing attackers to incorporate them into extensive botnet networks [65]. Cybercriminals are increasingly targeting smart devices due to their often inadequate protection and susceptibility to hacking. This makes them attractive instruments for executing powerful cyber

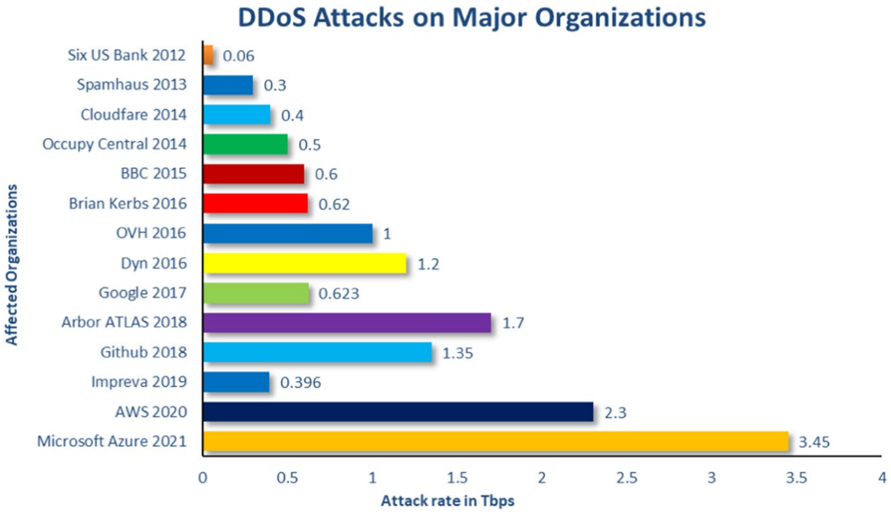

Fig. 7 Large scale DDoS attacks against major organizations [57–60]

attacks. Consequently, attackers frequently utilize these IoT botnets to carry out large-scale DDoS attacks. For example, in 2016, the Mirai malware utilized more than 2.5 million IoT devices as botnets to execute a large-scale DDoS attack on Dyn's DNS infrastructure [66]. This attack affected the world's leading DNS provider and caused significant Internet service disruptions. In this type of attack, the intensity of attack traffic is directly proportional to the number of IoT devices available in the botnet. Further, the Mirai botnet source code has been released into the public domain, resulting in an exponential increase in the number of Mirai IoT botnet DDoS attacks [67].

2.4 Cyberattacks taxonomy for IoT platforms

In the literature, several researchers [23, 25, 33, 68] have proposed IoT-based cyberattack taxonomies. However, these taxonomies failed to provide a comprehensive and wide range of cyberattacks related to IoT environments. Further, a few authors [69–72] presented various security problems but failed to provide solutions to mitigate these security problems.

Mathonsi et al. [70] proposed an IoT platform-based security taxonomy that covers several network security issues and PCI rather than addressing attack categories. Further, Ram et al. [71] primarily focused on communication layer issues associated with connected cars. And Shepherd et al. [72] proposed a taxonomy for IoT security in healthcare systems that give an overview of security considerations but do not elaborate on DDoS attacks type and their impact.

In this article, we propose a comprehensive cyberattacks taxonomy for IoT platforms and characterize each class of taxonomy w.r.t. IoT layers. The proposed cyberattacks taxonomy for IoT platforms is shown in Figure ??. The attacker mostly breaches the security of each layer of IoT technology-based applications. Therefore, in the proposed taxonomy, we categorized the cyberattacks based on the basic three-layer architecture of IoT technology, such as the application, network, and perception-layer attacks.

2.4.1 Perception-layer attacks

This layer primarily interacts with hardware, such as sensors, RFID tags, and other devices for transmitting and receiving information through distinct communication protocols, including RFID, Zigbee, and Bluetooth. This layer is also known as the sensing layer [73, 74]. Generally, IoT devices are deployed at unmanaged locations anywhere in the world, where intruders can quickly gain access without any difficulty, making them susceptible to several security attacks [75]. In this layer, cyberattacks are broadly categorized into two types: Physical and Malformed attacks. Some of the most common cyberattacks related to the above-mentioned classes are discussed in the following:

1. **Jamming attack:** Among the most severe threats to the IoT enabled sectors, jamming attacks highly affect IoT networks by obstructing communications, degrading IoT device performance, and exhausting their energy supplies [76]. It makes the perception layer of the IoT stack a victim. It involves interference with radio frequencies of the network that causes node frequency jamming when multiple devices share the same frequency channel [77]. Further, a small jamming source can also jam specific network nodes by sending artificial jamming signals.
2. **Collision attack:** Data collision happens when two or more nodes send data simultaneously while sharing the same channel. In that case, the data could be impacted by packet collisions, resulting in a mismatch in the checksum, which might result in the data being incorrect and dropped [78]. Moreover, re-transmitting data every time a packet crashes could impose additional burdens on the source node and the network, causing a denial of service and exhausting the entire network resources [79].
3. **Sleep deprivation:** The attackers take advantage of the power constraints of IoT devices by delivering fake control packets to the victim node until it is exhausted. The processing of these packets depletes the devices' power supply, resulting in sleep deprivation attacks [80]. It is common for IoT devices to have their security process enabled after booting, which allows the attacker to launch an attack during the booting process.
4. **Side-channel attack:** Side-channel attacks (SCAs) extract information from a chip or a system by measuring and analyzing physical factors, including timing information, power consumption, execution time, and radio waves [81].
5. **Node capture attack:** Sensors (a.k.a. nodes) are highly vulnerable to node-capturing attacks. Attackers capture or replace malicious nodes in a node-capturing attack.
6. **Malicious input attack:** An attacker has the opportunity to inject malicious code or false data into the node while updating these node's firmware or software over the wireless medium, resulting in financial loss, excessive power consumption, and deteriorating performance of devices and networks [82].
7. **Eavesdropping:** A network that operates in an open environment puts its nodes at risk for eavesdropping attacks during data transfer or similar events [83].

Further, this layer is vulnerable to some other attacks like replay attacks, bluesnarfing, physical damage, etc (Fig. 8).

2.4.2 Network-layer attacks

This layer of the IoT architecture incorporates numerous functionalities, including routing, adoption, and fragmentation. It enables physical objects always be connected in IoT systems using network services, such as wired and wireless networks. Sensor networks play a vital role while designing IoT networks. Therefore, this layer is more likely to generate sophisticated attacks, ranging from route manipulation to fragmentation. It can impact the availability of network resources. It can be split into: (i) Protocol-based and (ii) Volume-based attacks [84]. Volume-based attacks can be sub-categorized into two types: low-rate and high-rate attacks. In high-rate DDoS attacks, the frequency is excessively high, whereas low-rate attacks have the same frequency as legitimate traffic.

The protocol-based attacks are also referred to as resource depletion attacks, as they consume the target server's resources (CPU, Memory) and communication tools (firewall, load balancer) [85]. They were quantified by packets per second (Pps). A few of the protocol-based attacks are presented in the following:

1. **LAND attack:** This attack aims to form an infinite loop. To launch a local area network denial (LAND) attack, an attacker sends a synthetic SYN packet to the victim system and sets the target IP as the source IP [86]. However, the target server recursively generates replies to this packet, resulting in a feedback loop. In this scenario, the target server may crash eventually due to a LAND attack [87, 88].
2. **ACK-PUSK flood:** TCP connections are established through a three-way handshake process that begins when the client transmits an SYN request to the server [89, 90]. After that, the client receives an SYN + ACK packet from the server. In the end, the client sends ACK to complete this process successfully. An attacker with malign intent can use multiple botnets to send an ACK, PUSH bit-enabled packet with a forged source address, and the target device will drop the packet due to the server not having a connection to the spoofed IP address [91–93]. It results in the complete exhaustion of the server's resources due to excessive processing of every incoming packet.
3. **Smurf attack:** This attack manipulates the Internet control message protocol (ICMP) using a malware strain known as Smurf. An attacker sends multiple ICMP packets originating from a spoofed source IP address and broadcasts them to all computers on the network through a broadcast address. It causes each node of the network to respond to the ICMP request. Therefore, a significant amount of traffic receives by the victim.
4. **SYN-ACK flood:** An attacker exploits the second step of the three-way handshaking process to perform an SYN-ACK flood attack. In this step, the attacker overwhelms the target server with multiple spoofed SYN-ACK packets using a botnet or spoofed IPs. Meanwhile, the target server attempts to handle these requests, which consumes considerable resources, including RAM and CPU, during excessive processing.
5. **SSDP flood:** An attacker exploits the Simple service discovery protocol (SSDP), a network protocol used to advertise and discover network services in small networks. Further, it supports Universal Plug-and-Play (UPnP) service in devices for sharing information through UDP. This attack involves transmitting small UDP packets containing the target server's spoofed IP address to multiple UPnP-enabled devices until the server becomes offline due to the flood of requests from these devices.
6. **Selective forwarding:** It is one of the most prevalent routing attacks. It drops specific packet data during transmission to construct a hole in the network. It is performed by forwarding only particular packets to the next node. If this attack is in tandem with a sinkhole attack, then it becomes more dangerous for the network.

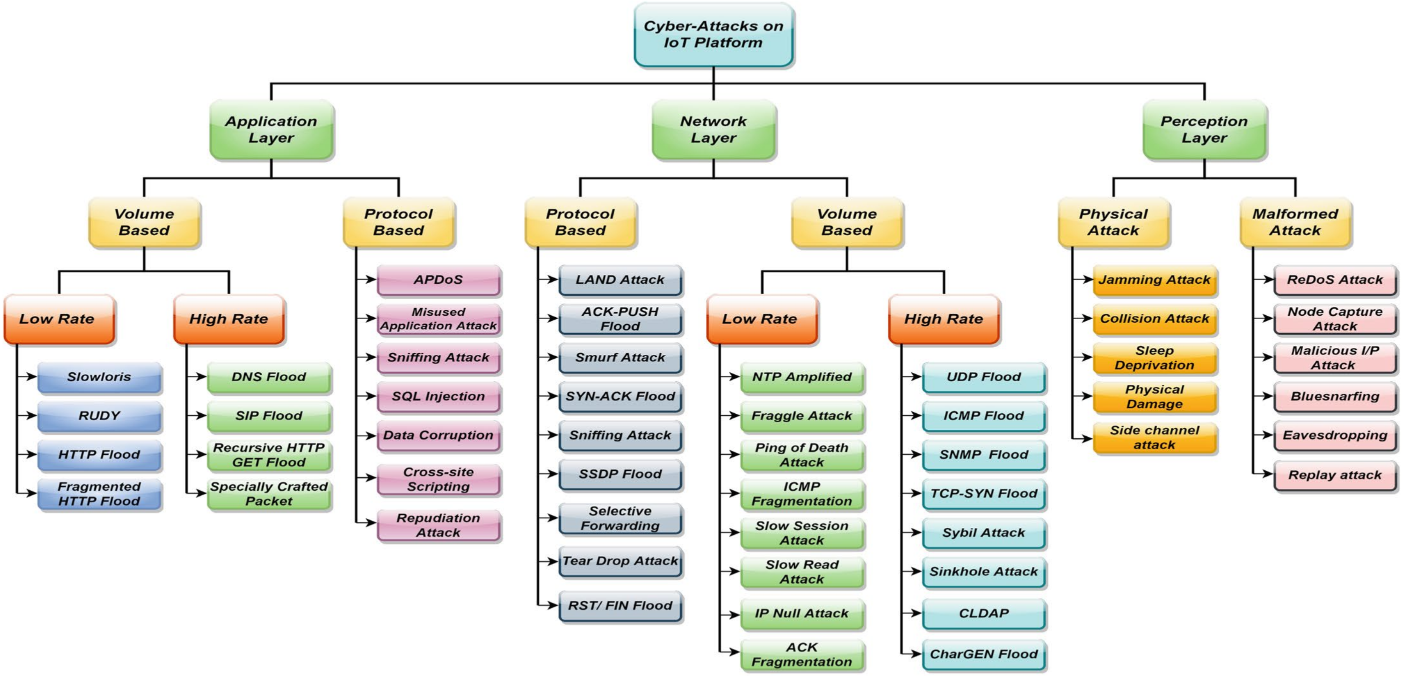

Fig. 8 A comprehensive cyberattacks taxonomy for IoT platforms

7. **Teardrop attack:** This attack happens when the malefactor transmits fragmented packets toward the target system [94]. Due to the vulnerability in TCP/IP fragmentation reassembly, the server system cannot reassemble such received packets. Therefore, fragmented packets overlap, and network devices crash due to this issue. It generally performs on outdated operating systems [95, 96].
8. **RST/FIN flood:** After growing three-way handshaking of the TCP-SYN session, the server exchanges RST or FIN packets to terminate the TCP-SYN session between the host and client. An RST or FIN flood attack affects a target server by receiving large numbers of RST or FIN packets from attackers who do not belong to the TCP-SYN session with a target server. The RST or FIN flood attack depletes a victim's firewall or servers by draining their system resources.

The volume-based attacks a.k.a. bandwidth depletion attacks. It immediately overwhelms a target server's bandwidth by generating an enormous amount of traffic. Some of the most popular volume-based attacks are presented as follows:

1. **NTP amplified:** Network time protocol (NTP)is used to synchronize the computer's clock with the server over the Internet. Malefactor exploits NTP to perform the NTP-amplified attack. This attack occurs when the attacker transmits amplified data packets (monlist command enabled) to the NTP server through a pool of spoofed IPs of the target [97, 98]. The target NTP server starts responding to every request, and the high frequency of responses overburdens the network's bandwidth. Therefore, it results in the denial of legitimate requests.
2. **Fraggle attack:** Fraggle attacks a.k.a amplification attacks. It floods the victim network bandwidth using UDP_ECHO_PACKETS instead of ICMP echo reply packets [99]. In this attack, attackers employed reflectors as a launching pad to transmit large amounts of spoofed UDP packets to the broadcast IP of the network. It resulted in a turndown of service.
3. **Ping of death:** In this attack, attackers transmit ICMP echo requests that exceed the conventional IP packet-size limit and cause the victim's server to freeze or crash. Typically, the maximum length of an IP packet is 64 Kbytes. It is necessary to break down large IP packets into smaller fragments and reassemble them on the recipient's side, forming a larger IP packet than 65535 bytes [100]. As a result of this inconsistency, the computer system allocated several resources for assembling the faulty packets. An attacker can consume network bandwidth and makes the network offline.
4. **IP Null attack:** This attack involves sending a spoofed IP packet with an IPv4 header that indicates which transport protocol is used. In this type of attack, the attacker assigns the value to zero for this field. Therefore, this type of packet is overlooked by the security mechanism (firewall), although they are designed to scan TCP, UDP, and ICMP. When the target server is overburdened with these packets and attempts to handle them, it may eventually lead to a system crash.
5. **UDP flood:** In a UDP flood attack, the attacker attempts to recursively transmit multiple UDP packets with spoofed IPs to the different ports of the victim system. In the meantime, the victim system inspects each port repeatedly for a piece

of application information but finds no such program. As a result, the victim system sends ICMP (Destination unreachable) packets as the suitable response to the spoofed IP address, whereas it does not receive any response from the attacker's side. [101].

6. **ICMP flood:** This attack aims to render Internet congestion by consuming the network bandwidth, and due to this, the target system denies access to legitimate users [102]. Attackers transmit numerous ICMP requests to a broadcast station using spoofed source IPs to exhaust the victim's server bandwidth [103].
7. **SNMP flood:** SNMP flood attack exploits the functionality of Simple network management protocol. SNMP is primarily used to manage network devices like servers, hubs, switches, and routers. In an SNMP attack, the hacker transmits numerous SNMP requests with spoofed IPs (of the victim system) to multiple network devices. Therefore, these devices respond to the victim system with a large number of response packets.
8. **SYN flood:** In SYN flood, the attacker exploited the functionality of TCP protocol by sending SYN packets with forged IPs toward the targeted system to initiate the connection establishment process. In order to confirm the connection, the victim system responds with SYN+ACK packets and waits for ACK packets. However, the attack devices didn't send the ACK packets to the victim system. Therefore, the connection is opened and waits for the ACK packets for a long time [104].
9. **Sybil attack:** This type of attack is also called an identity fabrication attack. In this, the primary objective of the attacker is to identify vulnerable nodes for obtaining unauthorized access to IoT networks. Further, vulnerable nodes attempt to promote themselves as another node in the network by stealing or falsifying the identity of other nodes [105]. Once attackers get control of the network, they modify routing protocols and disrupt overall network administration. This attack also reduces systems effectiveness and network performance [106].
10. **Sinkhole attack:** The attacker compromises several nodes from the IoT network to perform DDoS attacks [107]. The malicious node attempts to gain the attention of neighboring nodes by advertising its superior rank over its parent nodes. It yields the adjacent nodes to revise their parent node and modify the routing table. As the sinkhole node becomes the parent node and all the nearby nodes revise their routes to pass through the sink because the attacked node announces a better-fabricated route.

2.4.3 Application-layer attacks

In the case of application-layer attacks, the application or web server is overwhelmed with false requests. It led to denying access to legitimate packets. Attackers generally perform this type of DDoS attack by flooding numerous HTTP requests (get/post) to the victim system or applications. The magnitude of this attack is measured using requests per second (Rps) [108]. Application-layer attacks are broadly categorized into protocol-based and volume-based attacks. Further, volume-based attacks can be sub-categorized into low-rate and high-rate attacks.

The most popular volume-based application-layer attacks are presented in the following:

1. **Slowloris attack:** Slowloris is one of the variants of HTTP traffic-based DDoS attacks. It is an uneventful attack that opens numerous HTTP connections of the target web server. Further, an attacker sends the partial HTTP request at regular intervals to keep the connection open for an infinite time. Therefore, the resources of the target system are gradually consumed until they are completely exhausted, and then the server starts discarding all legitimate requests. It is challenging to protect the target system from this type of attack [109].
2. **RUDY attack:** The R.U.D.Y. (R-U-Dead-Yet?) attack is a famous denial-of-service attack. It is a slow-rate attack like Slowloris and submits long-form data at a slow speed to bring down a web server. It is also known as a "low and slow" attack since it forms a small number of long requests instead of overloading a server with multiple instant requests. In this, hackers open a limited number of sessions to the targeted server or website over a short period, leaving them open as long as possible, eventually exhausting all its connections [110].
3. **HTTP flood:** HTTP flood attacks are the most commonly used DDoS attacks for performing attacks on the application layer. In this attack, attackers created a massive network (i.e., botnet) of compromised devices called bots. With this botnet, attackers overwhelm web server(s) with numerous legitimate HTTP requests and force the server to preserve maximum resources to process these requests [89].
4. **DNS flood:** In this type of DDoS attack, the attackers exploited the functionality of the DNS. DNS amplification attacks are volumetric DDoS attacks. It exploits open DNS resolvers by sending a large number of DNS lookup requests with a spoofed source IP of the victim. Therefore, the DNS server process these requests and sends responses to the target system [111]. Typically, a small DNS request can result in a high volume of DNS responses.
5. **SIP flood:** The goal of this attack is to bombard the SIP REGISTRAR or the SIP registration server with spoofed requests. It exhausts all resources, including network bandwidth, processing capacity, and storage [112]. This attack will potentially overwhelm the server, resulting in a service outage and couldn't provide uninterrupted service for legitimate users.
6. **Specially crafted packets:** Attackers employing specially crafted packets exploit poorly developed websites, vulnerable web applications, or improper binding with databases to bring the servers offline. Further, they created different data packets for lock-up database queries. These attacks are particularly persuasive since they consume extensive resources of the target server. A single attacker typically launches them. An instance of a Specially crafted DoS attack is MS13-039.

Sometimes, attackers exploit the vulnerability in the application layer protocols. It results in exhausting the CPU and memory resources of the victim system or application. The most common protocol-based application-layer attacks are presented in the following:

1. **APDoS attack:** Advanced Persistent DoS (APDoS) is a threat posed by attackers who like to drive extreme destruction to the target system or application. It combines the most powerful features of state-of-the-art attacks and multivector approaches for targeting each component of the application layer. It is a threat that extends beyond simple flooding attacks.
2. **Misused application attack:** Instead of using bots to overwhelm the victim server, the attacker redirects traffic of heavily loaded applications, like peer networks (P2P network services) from legitimate clients to the target server. Therefore, the server goes down because of the immense processing load of numerous requests from multiple legitimate users.
3. **Cross-site scripting:** When a user is connected to a trusted website through a browser, the cross-site scripting attack can execute arbitrary code in their browser. This attack uses a user application as the conveyance. In this, the browser does not know about the malicious code, it proceeds to download the script code from an authorized website. The security zones in Internet Explorer do not provide any protection. Therefore, user authentication cookies are usually accessed by the malicious code stored in the local computer.

3 Review methodology

The primary objective of this study is to provide comprehensive learning of IoT traffic-based DDoS attacks, characterization of various IoT traffic-based datasets, and critical analysis of the existing detection approaches, challenges, and their feasible solutions. To achieve this:

1. We adopted a systematic literature review methodology to conduct this comprehensive review. Further, analyzes recent researches and future trends related to IoT security by examining the most significant and recent publications from 2020 to 2022.
2. We will explore various ML and DL-based attack detection approaches used in the literature by researchers for classifying network traces into benign and malicious traffic patterns.

There have been several surveys in the domain of IoT security that have covered different aspects. However, most existing systems were neither systematically carried out nor centered on ML and DL-based techniques. Therefore, this systematic literature review mainly focused on critically analyzing the existing approaches to protect Internet services from distributed and wide-scale IoT traffic-based attacks.

3.1 Search strategy

Applying an appropriate search strategy is the initial stage of the systematic review process. Further, finding relevant studies that match the research topic is a highly critical step in the review process. Therefore, a comprehensive group of databases has been compiled to extract the relevant literature.

We have searched the following digital libraries for this research work: ACM digital library, Science Direct, IEEE Explore, Wiley, Springer, and Google Scholar.

Further, we performed a pilot study to recursively refine the search string to achieve our research objective and retrieve articles related to IoT security or large-scale DDoS attacks in digital databases. The following search query is common for all digital library collections, with some minor modifications: IoT traffic-based DDoS attacks or DDoS attacks in IoT networks. The number of results obtained from the databases was analyzed for refinement by the "selection process," as demonstrated in Fig. 9.

3.2 Research selection process

This paper presents a systematic approach to the comprehensive literature review that identifies specific criteria for filtering research articles that do not fulfill our research goal. As a result, we have few more focused and recently published research articles on IoT and ML or DL-based techniques available in the literature to detect large-scale IoT traffic-based DDoS attacks. A detailed description of the research selection process is as follows:

- The process begins with collecting research articles based on the keywords seen in the titles or abstracts of the articles in search engines.
- In the initial screening, articles are filtered based on including and excluding criteria described in the next Sects. 3.2.1 and 3.2.2
- We exclude unrelated articles on IoT security at the first filtration level by simply reading the titles.
- The second filtration level is to filter out articles unrelated to the IoT traffic-based DDoS attacks by reading the abstract.
- During the third stage, we read the full text of the articles and removed those papers that have no relevance to ML/DL-based approaches to detect IoT traffic-based DDoS attacks.

3.2.1 Inclusion criteria

- Articles that provide IoT security solutions: preventing IoT systems from DDoS attacks.
- All research paper focuses on ML/DL-based approaches to analyze IoT network traffic to recognize large-scale DDoS attacks.

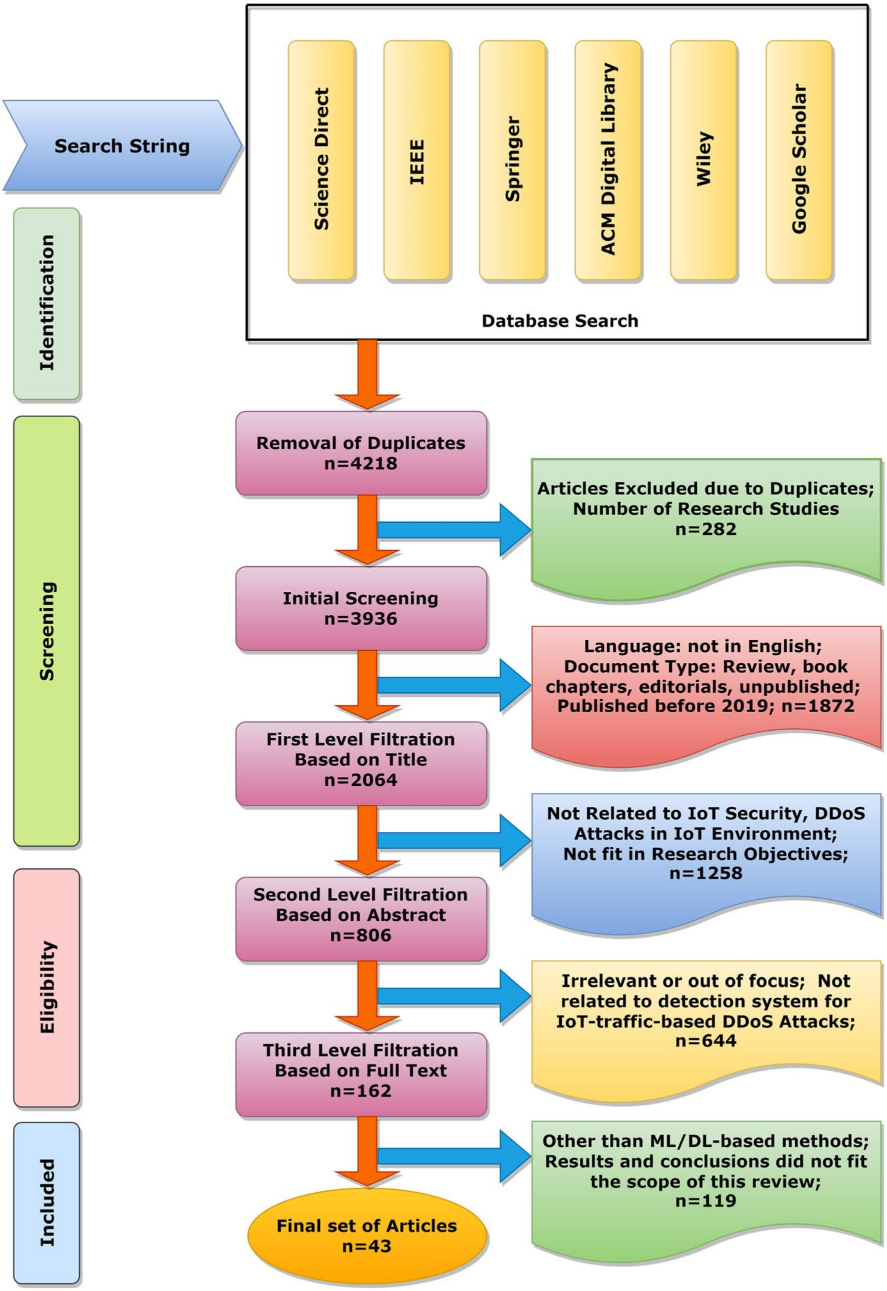
Search String
Science Direct
IEEE
Springer
ACM Digital Library
Wiley
Google Scholar
Database Search
Identification
Screening
Eligibility
Included
Removal of Duplicates n=4218
Articles Excluded due to Duplicates; Number of Research Studies n=282
Initial Screening n=3936
Language: not in English; Document Type: Review, book chapters, editorials, unpublished; Published before 2019; n=1872
First Level Filtration Based on Title n=2064
Not Related to IoT Security, DDoS Attacks in IoT Environment; Not fit in Research Objectives; n=1258
Second Level Filtration Based on Abstract n=806
Irrelevant or out of focus; Not related to detection system for IoT-traffic-based DDoS Attacks; n=644
Third Level Filtration Based on Full Text n=162
Other than ML/DL-based methods; Results and conclusions did not fit the scope of this review; n=119
Final set of Articles n=43

Fig. 9 A research selection process for systematic literature review

- The most suitable and scholarly publications on subjective analysis includes suitable methods, outcomes, or datasets.
- Research studies that contribute to the objectives of this review article.
- Research that extends previous related work.
- The papers were published from 2020 to 2022.

3.2.2 Exclusion criteria

- Document type: Unpublished, review articles, book chapters, grey literature, editorials, meta-analysis, software documentary, keynote, tutorial.
- Language: Full text in other than English.
- Availability: Inability to access the full article.
- Not appropriate methods or datasets used for subjective analysis is unrelated to the research topic.
- Studies with irrelevant results and conclusions did not fit the scope of this review.
- Duplicate research articles.

3.3 Data extraction

After completing a stringent selection process in the above mention section, a refined set of articles was left out for further analysis. Data extraction from selected research papers needs in-depth analysis, identification, and gathering of essential information. Further, we assemble critical and valuable data from each study into a pre-designed format. It consists of different fields: key references, attack detection methods, ML/DL algorithms, datasets, nature of the dataset (imbalanced/balanced), experimental setup, number of attack classes or features, pre-processing techniques, feature selection methods, results (accuracy), limitations, and observations. The details of fields are displayed in Table 6.

4 Review of existing approaches to detect IoT traffic-based DDoS attacks

Several researchers have proposed IoT traffic-based DDoS attack detection approaches in the literature. However, traditional systems failed to provide a complete solution for protecting Internet-based services/IoT networks from large-scale IoT traffic-based DDoS attacks. Further, the widespread integration of IoT devices in every sector with minimum security features increases the frequency of DDoS attack incidents. In the literature, few researchers proposed ML and DL techniques-based detection approaches. This type of system at least provides high-accuracy solutions against DDoS attacks compared to traditional solutions. In this section, we systematically analyzed the existing detection approaches. Therefore, we divided this section into two subsections: ML and DL techniques-based solutions to detect IoT traffic-based DDoS attacks.

4.1 Review of ML technique-based methods to detect IoT traffic-based DDoS attacks

ML technique-based approaches strengthen the security for Internet-based services and IoT networks from different types of cyberattacks by embedding intelligence. Various ML-based algorithms are employed to design ML-based detection models for identifying different types of attacks. Several ML-based detection approaches are available in the literature, and we systematically examine them in the following:

Soe et al. [113] proposed an IoT-botnet attack detection approach using a sequential attack detection framework. They employed three ML algorithms: the J48 Decision tree, Naive Bayes, and ANN classifier. Researchers have claimed that this approach has given 99% classification accuracy. They designed the proposed approach using the N-BaIoT dataset. This system consists of two phases: (i) "Model Builder" and (ii) "Attack Detector". In the first phase: data collection, data organization, model training, and feature selection were conducted. In the second phase, analyze the incoming traffic and determine whether it is normal or attack traffic. The primary purpose of this approach is to classify network traces into binary classes:

Table 6 Relevant fields for data extraction

Field	Functionality
Key Reference	Provides Author’s name, research paper title, and year of publication
Attack detection methods	List the different approaches utilized for detection of large-scale DDoS
	attacks in the paper
ML/DL Algorithms	Provide a list of different ML/DL models used in the paper
Datasets	Give information about different datasets used for evaluation in the study
Nature of the Dataset	Dataset type (Imbalanced/Balanced)
Experimental setup	Provide knowledge of hardware and software requirements, performance
	parameter used by researcher in the paper
No. of attack classes or features	List various attack classes including benign, no. of features exist
Pre-processing techniques	Depict Pre-processing techniques used by researcher to prepare data
	before model training
Feature selection methods	List various feature selection methods, to reduce computational cost and improve accuracy of the model
Results (Accuracy)	Provide final outcomes of the study, to compare with the existing model
Limitations	Provide gaps and open issues, of the research paper
Observations	Final concluding remarks about the above fields

legitimate and attack. However, this approach failed to distinguish different categories of DDoS attacks.

Lawal et al. [114] proposed a DDoS attack mitigation framework in fog computing for detecting attacks more accurately. They utilized three ML-based techniques for implementing this approach: DT, NB, and KNN. Further, they have classified network traces into two classes: legitimate and attack. This system is designed using the CICDDoS 2019 dataset. The authors claimed that the performance of the KNN classifier delivers a higher classification accuracy of 99.9% than others. However, the proposed system failed to protect the Internet-based system from IoT traffic-based DDoS attacks traffic flows.

Shafiq et al. [115] proposed a novel framework model with a practical feature selection approach named CorrAUC. This framework is specially designed to identify anomalies and malicious traffic in the IoT network. They used the AUC metric, Pearson correlation, and the class label to estimate each feature's significance. By using these methods, choose the 5-best features and design ML-based model using these features. The author evaluated four ML-based approaches on the Bot-IoT dataset: DT, SVM, RF, and NB. They claimed that the DT-based model has given better classification accuracy (approximately 99%) than other methods. The primary focus of this approach is to protect the victim from DoS attacks, and it has failed to provide a better solution against large-scale DDoS attacks.

Doshi et al. [116] proposed an IoT traffic-based DDoS detection approach for identifying large-scale IoT traffic-driven DDoS attacks. Firstly, they create the feature vector by dividing network features into stateless and stateful features. The stateless features include packet header fields, such as packet size and protocol. The stateful features collect flow information, such as bandwidth, source IP, and destination IP. Secondly, these features feed to the different machine learning techniques (LSVM, KNN, DT, RF, NN) for designing the detection model. They claimed this system efficiently classifies incoming traffic into legitimate and attack traffic with 99% accuracy. However, the results obtained from this system might be biased towards the majority class due to it being designed using an unbalanced dataset. On the other hand, powerful botnets like Mirai frequently mutate, making them difficult to identify.

Churcher et al. [117] employed different ML techniques: KNN, SVM, DT, NB, RF, ANN, and LR, for implementing their detection approach. They designed this system using a realistic Bot-IoT dataset. Further, They used 1.5 million records to test the performance of this system. The KNN-based approach performs well with a classification accuracy of 99%. However, this system is designed using unbalanced data and may produce inaccurate results in a real-world scenario. Further, this approach is failed to distinguish between a flash event and DDoS attacks traffic flows. In Table 7 and 8, we systematically characterize and summarize the detailed review of recent ML-based approaches based on various parameters: attack detection methodology, the dataset used, attack classes, experimental setup, number of features utilized, feature selection methods, and feature engineering strategies.

4.2 Review of DL technique-based methods to detect IoT traffic-based DDoS attacks

Nowadays, deep learning techniques are widely employed for providing solutions to various critical problems. In this, models are designed using large amounts of prepared data/ patterns and predict output more accurately based on their learned experience. In the case of DDoS attacks, models are responsible for predicting legitimate traffic, different types of attacks, and flash events by analyzing incoming network flows. Further, DL-based approaches offer high-accuracy solutions. Therefore, several researchers proposed DL-based detection approaches for protecting the IoT environment against large-scale cyberattacks. This type of approach helps us to improve the precision of the model. In this section, we characterize existing DL-based detection approaches, and they are presented in the following:

Larriva et al. [140] proposed DL-based IDS approach for protecting the IoT networks. They used different datasets for creating their models: UNSW-NB15, UGR16, and NSL-KDD. They employed z-score, min-max, and distinct pre-processing schemes on these datasets with predefined classes. They employed MLP-Classifier for classifying network flows. The classification accuracy of this system is 99.7%+, 99.2%+, and 99.3%+ for NSL-KDD, UNSW-NB15, and UGR16, respectively. However, the comparative analysis of the proposed system's performance w.r.t. attack types is not presented. Further, this approach failed to distinguish between a flash event and DDoS attacks traffic flows.

Popoola et al. [141] proposed a DL-based approach for detecting botnet attacks in IoT networks. They used a highly imbalanced Bot-IoT dataset to develop this detection approach. Therefore, the synthetic minority oversampling (SMOTE) technique is employed to balance out asymmetric network traffic data in the Bot-IoT dataset and minimize overfitting or underfitting problems. Further, after normalizing the data, they implemented the DRNN model. The proposed models efficiently classify the majority classes (DD_T, DD_U, D_T, D_U, OSF, and SS). However, no feature selection technique was employed while designing this detection approach. Therefore, it will require more time to collect all features. Further, it becomes a victim during a large-scale attack.

Hezam et al. [153] proposed a DDoS botnet attack detection approach that combines BiLSTM and CNN models. They have given a solution to detect the most destructive Mirai and Bahlite botnet-based DDoS attacks. This approach consists of two parts: (i) By employing CNN for pre-processing and feature optimization tasks and (ii) The BiLSTM for detecting DDoS botnets in the network. This approach is validated using a realistic N-BaIoT dataset comprising attack traffic from nine infected IoT devices. The performance analysis of four DL-based models (such as CNN, RNN, LSTM-RNN, and BiLSTM-CNN) executed using a tenfold cross-validation technique. It has been viewed that the BiLSTM-CNN model performs better than other models. However, the BiLSTM-CNN model uses full features to detect botnet attacks, but its accuracy is not enough to deal with today's highly-frequent and complex cyberattacks.

Koroniotis et al. [154] proposed a DL-based attack detection technique. The authors have designed three ML/DL-based detection models with LSTM, SVM,

Table 7 Summary of recent ML-based attack detection approaches, their feature selection and feature engineering strategies

Authors	Year	Dataset	Feature Engineering	Feature Selection	Key points
Aysa et al. [118]	2020	Synthetic dataset	Min-max normal- ization, drop al redundant data	Pearson coefficient correlation	Lightweight detection model with high accuracy is designed with a correlation-based feature selection
Ullah et al. [119]	2020	IoT-Botnet	Used min-max normalization to get all feature values on the same scale	Recursive feature elimination technique	Generated IoT botnet dataset provides flow-based features used to analyze and evaluate the IDS for IoT efficiently
Soe et al. [113]	2020	N-BaIoT	Min-max normalization	Correlation-based approach	Lightweight detection model with high accuracy is designed with a correlation- based feature selection
Samdekar et al. [120]	2021	Bot-IoT	Encoding categorical features, merging of similar data, drop all constant features	Extra tree classifier, Chi2, PCA firefly algorithm	The accuracy of the proposed system is improved with dimensionality reduction methods and also reduces over-fitting issue, computing cost
Pokhrel et al. [121]	2021	Bot-IoT	Data cleansing, Min-max normalization, Data transformation to convert categorical features into numerical	F-Score (Chi2 value)	This study exhibits that the KNN algorithm efficiently detects botnets in IoT networks
Seifousadati et al. [122]	2021	CICDDoS 2019	Encoding categorical features, drop all correlated, constant features	Features' importance	Essential features are selected as having the highest importance value for detecting DDoS attacks
Nimbalkar et al. [123]	2021	Bot-IoT KDD Cup 1999	Remove duplicates, NaN and missing, values are replaced with zero to get compact dataset	Information gain (IG), Gain Ratio (GR)	The system achieved higher detection rates using IG and GR feature selection methods with the top 50% ranked
Das et al. [124]	2022	CSE-CIC-IDS2018	Feature Scaling using MinMaxScaler, and drop NaN, insignificant feature values	ANOVA F-test, Recursive, Feature, Elimination	This study indicates that the feature selection can be used to reduce training

Table 7 (continued)

Authors	Year	Dataset	Feature Engineering	Feature Selection	Key points
Alduailij et al. [125]	2022	CICIDS 2017, CICDD0S 2019	Convert non-numeric into numerical values, removing irrelevant or corrupted data records	MI RFFI methods	Both selecting best and new feature generation helps in improving performance of ML models
Shukla et al. [126]	2023	Bot-IoT	Convert non-numeric into numerical values, removing traffic flows which are having inco- mplete or NAN values	Embedded feature reduction method	The proposed method higher detection rate using embedded feature reduction method and also minimize overfitting issue

and RNN algorithms using the IoT dataset (synthetic dataset created while doing this research). For implementing these models, the top 10 features were extracted from the synthetic dataset using statistical techniques: correlation coefficient and joint entropy. However, they failed to evaluate the adversarial robustness of these DL-based models. Further, the primary focus of this approach is to classify network traces into two classes: attack and legitimate. Therefore, it failed to distinguish between different DDoS attacks.

Kim et al. [155] proposed a deep neural network (DNN)-based approach for protecting networks from a broad range of security threats. This approach designed using the KDD-1999 dataset. In the proposed method, two variables are employed for intrusion detection consisting of four hidden layers and 100 neurons in each hidden layer. They used a ReLU activation function combined with stochastic gradient descent (SGD) optimization function. The author claimed that the proposed model efficiently classified network traffic with 99% accuracy. However, the proposed approach failed to protect the victim's system from large-scale DDoS attacks.

Feng et al. [156] proposed a DL technique-based model to classify different security threats and DoS attacks. They employed both CNN and LSTM models as classification techniques to identify security threats by XSS and SQL. This approach is designed using the well-known KDD-CUP 99 dataset. The sample data (collected data) is divided into two parts: 70% for training and 30% for testing. This approach helps us to detect XSS attacks through DNN and CNN with 57% and 78% accuracy, respectively. However, this approach primarily focused on protecting Internet-based services from DoS attacks and failed to identify large-scale DDoS attacks.

In Table 9 and 10, we systematically characterize and summarize the detailed review of recent DL-based approaches using various parameters: attack detection methodology, the dataset used, attack classes, experimental setup, number of features utilized, feature selection methods, and feature engineering strategies.

Table 8 Summary of recent ML-based attack detection approaches with their attack detection methodology, the dataset used, experimental setup, classes of attacks classified, and the number of features utilized

Authors	Year	Dataset	Attack Detection Methodology	Classes of Attacks Classified	Experimental Setup	Performance Evaluation (%)	Features Utilized
Dwivedi et al. [127]	2020	KDD Cup 99 CONFICKER worm	DT(C4.5), SVM, NB, MLP	Distributed Denial-of-Service, Benign	–	Accuracy: KDD Cup 99 C4.5=99.25,SVM=98.27 NB=69.84,MLP=88.57 CONFICKER wormsC4.5=98.35,SVM=97.34 NB=72.37,MLP=89.38	Full
Rani et al. [128]	2020	NSL KDD KDDCUP99	KNN, LR, NB, DT, RF	Normal, DoS, Probe, User to Root, Remote to Local	Python version 3.7.4 with commonly used like: pandas, sklearn, numpy	Accuracy: KDD CUP 99 RF=99.9, KNN=99.8, NB=91.9, DT=99.9, LR=97.1; NSL KDD: RF=98.1, KNN=96.8 NB=36.3, DT=98.0	10
Chen et al. [129]	2020	Generated dataset	Multi-layer DDoS detection system	Normal, DDoS ICMP, DDoS SYN, DDoS UDP, Sensor data flood	The 5 distinct sensors are distributed among 8 smart poles, and a Heterogeneous gateway, Raspberry Pi 3, used to transmit and receive packets form smart poles	Accuracy: Sensor data flood=97.39 Network data flood = 99.98	Full
Chesney et al. [130]	2020	CICDDoS 2019	Logistic regression	NetBIOS, Benign LDAP	A laptop with 32 GB RAM, runs 64-bit Windows OS, and CPU speed of 2.8 GHz Python version 3.7.4 with Scikit-Learn, Matlplotlib, Pandas, Seaborn, libraries	Accuracy of Logistic regression=99.7	5
Syed et al. [131]	2020	Generated dataset	AODE, C4.5, MLP	Normal, MQTT-DOS-BF1, MQTT-DOS-BF2, MQTT-DOS-BF3, MQTT-DOS-IAUTHS, MQTT-FUZZ, TCP-DOS	2-physical servers, Raspberry Pi 3, WEMOS ESP8266 devices, 2-wireless routers	Accuracy: AODE=99.84, C4.5=99.82, MLP=84.22	28

Table 8 (continued)

Authors	Year	Dataset	Attack Detection Methodology	Classes of Attacks Classified	Experimental Setup	Performance Evaluation (%)	Features Utilized
Churcher et al. [117]	2021	Bot-IoT	KNN, DT, RF, NB, SVM, LR	Data exfiltration, DoS TCP, Benign,DoS HTTP,DoS UDP, DDoS HTTP, DDoS TCP, DDoS UDP, Keylogging, OS Scan, Service Scan	Python version 3.7.4 for implementing ML models, and two famous modules, scikit-learn and Keras, are used	Accuracy of ML models: KNN=99.0, DT=96.0 RF=95.0, NB=94.0 SVM=79.0, LR=74.0	19
Ahmad et al. [132]	2021	UNSW-NB15	Random forest, Support vector machine, Artificial neural networks	Normal, Exploits, Generic, DoS, Analysis, Shellcode, Reconnaissance, Fuzzer, Backdoor	Computer equipped with Processor: Intel (R) Xeon (R) CPU E3-1285 v6 @4.10 GHz with 8 CPUs, 4 cores per CPU, and has 2 threads per core. Runs with Ubuntu 18.04.1 LTS and holds 64 GB of RAM tool to run ML models	Accuracy: RF=97.37 SVM=95.67 ANN=91.67	Full
Alzahrani et al [133]	2021	CICDDoS	KNN, DT, RF, NB, SVM, LR	DNS, LDAP, MSSQL, NetBIOS, NTP, SNMP, SSDP, SYN, TFTP, UDP, UDP_Lag	Computer equipped with Intel® Core™i7-8650U CPU @ 1.90 GHz processor, runs with 64-bit Windows 10 (OS) and 16-GB RAM. Software WEKA version 3.9.4	Accuracy of ML models: KNN=98.0, DT=99.0 RF=99.0, NB=45.0 SVM=86.0, LR=98.0	24
Anwer et al [134]	2021	NSL KDD	SVM, RF, GBDT	Malicious, Benign	System manufacturer Lenovo,Processor:4500U, with 8GB memory, operating system:Ubuntu 20.04, attached NVIDIA graphic card, Python with libraries	Accuracy: SVM=32.38, RF=85.34, GBDT=78.01	Full
Krishnan et al [135]	2021	IoTID20	SVC, XGBoost, RF	Normal, Anomaly	Python programming-language with functional Libraries: sklearn, numpy	Accuracy: Recursive feature elimination SVC=98.76, RF=99.78 XGBoost=99.79	32

Table 8 (continued)

Authors	Year	Dataset	Attack Detection Methodology	Classes of Attacks Classified	Experimental Setup	Performance Evaluation (%)	Features Utilized
Kumar et al [136]	2022	Bot-IoT	DT, RF, NB, KNN, Stacked (DT,KNN,RF)	DDoS TCP, DoS, DDoS UDP, Benign	Testbed consists of 6-PCs, 2-smartphones, 2-routers, 4-sensor nodes, 6-sensors, Software: Argus, Python, Wireshark, LOiC, CMD	Accuracy: DT=98.59 RF=98.75 KNN=99.46 NB=74.27 Stacked=99.61	Full
Saghezchi et al [137]	2022	Generated from a semi-conductor production factory	LR, NB, SVM, BN, OneR KNN, DT, RF K-Means, EM	Malicious, Benign	–	Accuracy: RF=99.9 DT=99.9, SVM=97.1 NB=95.8, LR=97.0 OneR=98.7,BN=99.4 KNN=99.9,EM=95.0 K-Means=95.0	38
Gaur et al [138]	2022	CICDDoS 2019	KNN, DT, XGB, RF	UDP, LDAP, MSSQL, NetBIOS, Benign, SYN, UDP_Lag	The Google colab runs on Intel(R) Xeon(R) CPU with a frequency of 2.30 GHz and Ram of 12.72 GB, Cache size of 46 MB, Disk=0.10TB Software: Python 3.7.10. and Scikit learn 0.22.2	Accuracy of ML models: RF=85.05, DT=91.34 KNN=91.37, XGB=98.34	15
Amrish et al [139]	2022	CICDDoS 2019	KNN, RF, DT, ANN system	Benign, malicious	Programming-language Pyhton version 3.7.10 with libraries: pandas sklearn is used for implementing ML models	Accuracy: KNN=99.89, DT=99.50 RF=99.90, ANN=99.95	15

4.3 A detailed review of publicly available datasets

The solution to critical problems using artificial intelligence (ML and DL techniques) highly depends on high-quality data w.r.t. the number of records, accuracy in the data, selection of best features, balance data, etc. When the models are designed using asymmetric or inappropriate (non-IoT-specific) datasets, it may be possible models can give high performance during the training/testing phase. However, in a real-time environment, they fail to provide better accuracy. The comprehensive and benchmark dataset will help us to develop robust DL/ML-based classification models [167–175]. Therefore, we summarize various well-known and publically available datasets in this section. We systematically characterize them using different parameters in Table 11.

- IoTID20 [176] dataset is primarily employed to design IDS approaches. In this dataset, two intelligent devices are connected to the Wi-Fi router in order to simulate modern cyberattacks. Further, it includes 83 network traffic-related features, along with three additional features for labels: binary, category, and subcategory. It captures five attack categories: DoS, Mirai, scan, MITM, and legitimate. The number of instances in this dataset is 625,783 traces.
- ToN IoT [177] presents an innovative set of datasets for evaluating the effectiveness and reliability of various cybersecurity applications using Artificial Intelligence (AI). These datasets are referred to as ToN IoT due to the heterogeneity of the data collected from IoT and IIoT sensors' telemetry data, different operating systems' data, and IoT network traffic records.
- IoT-23 [145] is a recently published IoT network traffic-based dataset. It incorporates 20 malware classes and three benign classes captured during 2018-19. Further, this dataset assembles a massive number of instances for real and labeled (malicious attack and benign) flows captured from real IoT devices. The significant objective of this dataset is to provide a framework for developing ML-based intrusion detection mechanisms.
- MQTT-IoT-IDS2020 [178] is primarily used to develop IDS mechanisms to detect MQTT-based attacks. Message Queuing Telemetry Transport (MQTT) is a well-known "IoT machine-to-machine communication protocol". This dataset is generated by MQTT's simulated network architecture, including 12 sensors, a broker, a fake camera, and an attacker. Captured five different attack scenarios: "regular operation", "aggressive scanning", "UDP scanning", "Sparta SSH brute force", and "MQTT brute-force". It helps to differentiate between legitimate and malicious MQTT traffic.
- The MedBIOT [179] dataset is generated by designing a testbed. The testbed is a medium-sized network with 83 IoT devices (real and simulated devices). It is a labeled dataset that contains both legitimate and malicious IoT traffic collected from botnets. Three well-known botnets: Mirai, BashLite, and Torii deployed with the C &C.
- The IoTNID [180] dataset includes 42 PCAPs with raw network packets recorded at different periods. These PCAPs have 825,000 network flows, each instance consisting of seven features. In this dataset, there are five major categories and

eleven subcategories. Among the five major categories, one class is for legitimate transmissions, while the other four relate to cyberattacks.

- The CICDDoS2019 [181] dataset contains legitimate and different DDoS attack traffic flows. The network flows of this dataset are collected using a real-test-bed- environment for two days. On the first day, they conducted seven different types of attacks, while on the second day, they conducted twelve different types. This dataset is freely accessible to the research community in the following data formats: PCAP (without labeled) and CSV format (with 87 features, including labeled).
- A realistic Bot-IoT [154] dataset comprises legitimate and fabricated IoT network traffic with several attack types. The Bot-IoT dataset provides complete packet capture details, suitable labels, and approximately 72 million records. The source files of this dataset are publicly available in two data formats: PCAP and CSV, with sizes of (69.3 GB) and (16.7 GB), respectively. It contains eleven target classes and 46 features.
- N-BaIoT [182] comprises real IoT traffic data generated from nine commercial IoT devices. For collecting instances of this dataset, they employed two botnets, Mirai and BASHLITE. The malicious flows of this dataset are broadly categorized into two types, and these two are further sub-categorized into ten attack types with one benign class. This dataset is highly in-balanced due to the number of benign instances being minimal compared to malicious ones.
- The DS2oS [157] dataset includes application layer-based DDoS attacks collected from the IoT environment. In addition, it includes IoT middleware containing the data and services of intelligent spaces. Further, this dataset consists of 347,935 network flows with 13 different features, categorized into eight attack classes: Normal, Scan, DDoS, Multitious control, Multitious operation, Scan wrong setup, spying, and Data type probing.
- The CICIDS2017 [183] dataset includes legitimate and different cyberattacks. Each network flow of this dataset is marked as benign or one of the 14 different attack types. The CSV version of this dataset comprises 2,830, 743 network flows divided into eight files. Each instance of network flow consists of 79 features.
- The UNSW-NB15 [184] dataset includes 49 features and ten target classes, including benign. Several researchers utilize this dataset to develop protection mechanisms for devices and networks against malignant attacks. This dataset was created in a synthetic environment by performing simulated attacks. It comprises roughly one hour of anonymized network flows of different DDoS attacks.

4.4 Performance evaluation metrics

In this section, we present key standard performance metrics commonly employed to validate the effectiveness of cyberattack detection mechanisms. The widely used performance metrics include Accuracy, Precision, True positive rate, False positive rate, False negative rate, True negative rate, and F-measure. Furthermore,

Table 9 Summary of recent DL-based attack detection approaches, their feature selection and feature engineering strategies

Authors	Year	Dataset	Feature Engineering	Feature Selection	Key points
Dutta et al [142]	2020	IoT-23 dataset	Prepared the dataset and use DAE for finding minimal no. of features	Deep Auto Encoder	They employed mLSTM model on the IoT-23 dataset to evaluate the efficacy of the
Roopak et al [143]	2020	CICIDS 2017	Normalized in range 0, 1. Drop all constant, irrelevant data records	NSGA-II-aJG algorithm	For classification purposes the CNN integrated with LSTM gives better results with reduced feature set
Meidan et al [144]	2020	Generated dataset	Encoding categorical features, removing all constant, irrelevant correlated features	Feature importance by LGBM	The accuracy of the proposed system is improved with dimensionality reduction methods and also reduces overfitting issue, computing cost
Dutta et al [145]	2020	IoT-23 LITNET-2020 NetML-2020	A Deep Sparse Auto-Encoder is used for the feature engineering task during the initial step of data pre-processing	DSAE	Stacking ensemble-based strategy used for classification and its effectiveness is evaluated using a variety of realistic datasets
Haq et al [146]	2021	N-BaIoT	Drop duplicates, irrelevant, correlated Encoding categorical features	Principal component analysis	The use of PCA technique for feature extraction and enhance effectual and co-rrect Botnet detection in IoT environments
Ahmad et al [147]	2021	IoT-Botnet 2020	Remove the redundant and normalize values of all features, onehot-encoding for conversion	Mutual information technique	The use of information gain technique for dimensionality reduction enhance accuracy of the proposed anomaly detection mechanism

Table 9 (continued)

Authors	Year	Dataset	Feature Engineering	Feature Selection	Key points
Sharma et al [148]	2021	DARPA99	Bundles the packets into time-bound. Data transformation to windows	Principal component analysis	In this study, the fog layer used for detection of attacks and PCA for reducing features in the proposed anomaly detection architecture
Zeeshan et al. [149]	2021	Bot-IoT UNSW-NB15	Data type conversion, Drop missing, NAN values of all features	Information gain technique	The proposed PBDID-architecture, classifies attack traffic accurately by handling issues like imbalance and over-fitting
Wazzan et al [150]	2022	MedBIoT	Normalized by normal-standardizing all feature values ranges from 0 to 1	Statistical function approach	CNN-LSTM detection model designed to identify the IoT botnet with better accuracy than other models
shahhosseini et al [151]	2022	ISCX	Correlation vector	Automatic feature extraction	Automatic selection of relevant features from raw packet data enables DL-based analyzer to analyze network traffic correctly
Chaudhary et al [152]	2022	Generated dataset	Discretization and Min-max normalization	IG, CFS mRMF	New feature generation, as well as selecting best features, in-order to enhance performance of ML/DL models

we present some additional metrics, such as Geometric Mean (G-mean), and Matthews Correlation Coefficient (MCC), which are used in contemporary works.

4.4.1 Confusion matrix

The confusion matrix (CM) isn't an explicit performance metric in itself. However, it serves as a tool for determining the correctness of any classification model. The CMs parameters are used to calculate nearly all performance measures. It is shown

Table 10 Summary of recent DL-based attack detection approaches with their attack detection methodology, the dataset used, experimental setup, classes of attacks classified, and the number of features utilized

Authors	Year	Dataset	Attack detection	Classes of attacks	Experimental	Performance	Features
			Methodology	Classified	Setup	Evaluation (%)	Utilized
Latif et al [157]	2020	DS20S	ANN, SVM DT, RNN	DoS, Data type probing Malicious control Malicious operation Scan, Wrong setup Normal, Spying	Gaming-class computer:Dell-G5, Intel® Core™i7-9700 processor with CPU speed-4.7 GHz, DDR4 RAM-16GB NVIDIA GeForce-GTX-Ti-6 GB installed graphics card	Accuracy SVM=98.39, DT=99.08 ANN=98.55, RNN=99.20	11
Roopak et al [143]	2020	CICIDS2017	CNN, LSTM MLP, SVM NB, RF	Normal Abnormal	High-Performance Computer (HPC): GPU NVIDIA Tesla VIOO GPUs, having 16 GB VRAM with 256GB on 10 number of nodes in HPC Parameters: Hidden neurons 128, Learning rate:0.001	Accuracy CNNLSTM=99.03 MLP=88.74, SVM=94.5 NB=94.19, RF=93.64	15
Badamasi et al [158]	2020	CICDDoS 2019	Cuda-enabled LSTM	Normal, DDoS_DNS DDoS_LDAP DDoS_MSSQL	Computer equipped with 64-bit Windows 10 operating system with GPU-based seven score processors and RAM size is 16 GB Anaconda environment and python libraries	Accuracy Cu-LSTM=99.60	Full
Ahmad et al [147]	2021	IoT-Botnet 2020	DNN, CNN RNN, LSTM GRU	Anomaly Benign	HP laptop equipped with a OS Windows 10, 8 GB of RAM and CPU Intel Core I7-8550U, Graphic card NVIDIA GeForce MX150 Software: Python version 3.6.9, Google Colab online evaluation platform	Accuracy of proposed model DNN=99.01 RNN=98.43 CNN-1D=98.88 GRU=98.39 LSTM=96.41	16

Table 10 (continued)

Authors	Year	Dataset	Attack detection Methodology	Classes of attacks Classified	Experimental Setup	Performance Evaluation (%)	Features Utilized
Zeeshan et al [149]	2021	Bot-IoT UNSW-NB15	LSTM	Normal DoS DDoS	Hyper-parameter tuning The value of Dropout and recurrent dropout between 0 to 1, epochs:(1 to 10) and activation and recurrent activation value's are RELU, sigmoid, and tanh	Accuracy LSTM=96.32	26
Alkahtani et al [159]	2021	N-BaIoT	CNN-LSTM	Benign, Junk, Scan Mirai_udp, COMBO TCP, Mirai-Scan, ACK UDP, Mirai-SYN Mirai_udpplain	The computer with Windows 10 OS, i7 processor with 8GB RAM, Jupyter Python 3.6 and Matplotlib 3.2.0,Numpy 1.18.1, sklearn 0.22.1, Keras 2.3.1, TensorFlow 2.10	Accuracy of detecting doorbells attack=90.88 thermostat attack=88.53 security cameras=89.64	23
Ge et al [160]	2021	Bot-IoT	Feed forward neural network	Data exfiltration, DoS TCP ,DoS HTTP,DoS UDP DDoS HTTP, DDoS TCP DDoS UDP, Keylogging OS Scan, Service Scan Benign	A cluster of next-generation computers, one of which is Tesla V100 GPU and 93 G RAM Python with TensorFlow and Keras library	Accuracy Binary FNN=99.99 Multi-class FNN=99.79	29
Apostol et al [161]	2021	Bot-IoT	Deep Auto-Encoder	Normal Malicious	A computer with Intel Core i7 CPU, 16 GB RAM and NVIDIA GeForce graphic card. Python version 3.7.4 TensorFlow, Scikit-Learn and Pandas, libraries	Accuracy of Autoencoder with increased threshold=96.7 with initial threshold=99.7	10
Hezam et al [153]	2021	N-BaIoT	RNN, CNN LSTM-RNN BiLSTM-CNN	Benign, Junk, Scan Mirai_udp, COMBO TCP, Mirai-Scan, ACK UDP, Mirai-SYN Mirai_udpplain	Hyper-parameters: Batch size=1024, Input=115,1 Learning rate=0.001 Optimizer=Adam Epochs=100, Verbose=1	Accuracy RNN=89.77, CNN=89.50 BiLSTM-CNN=89.79 LSTM=89.71	Full

Table 10 (continued)

Authors	Year	Dataset	Attack detection Methodology	Classes of attacks Classified	Experimental Setup	Performance Evaluation (%)	Features Utilized
Cil et al [162]	2021	CICDDoS 2019	DNN	Normal Abnormal	A computer comprises Windows 10 OS, IntelCore i7-7700 K CPU 4.2 GHz processor, 32 GB RAM 2X512GB SSD and NVIDIA GTX 1080 Ti Graphics Co-processor Python 3.7 for implementation	Accuracy of proposed DMM model=94.57	69
Nasir et al [163]	2022	NSDLKDD	Deep neural network	Abnormal Normal	The system supports OS Ubuntu 18.04.2 LTS CPU Xeon E5/Corei5, RAM 128GB and GPU NVIDIA GeFroce 1080, TensorFlow version 1.x Software Python Version 3.7.4	Accuracy of proposed model DNN=99.23	14
Al razib et al [164]	2022	CICIDS 2018	Cu-DNNLSTM Cu-DNNGRU Cu-BLSTM	Benign, Brute-force, Bot DDoS-Hoic DDoS-Loic-Udp Infiltration	An Intel processor, Core i7-7700 supported by a Graphical Processing Unit. Software: Keras and 3.8 version of Python with vast libraries like Tensor Flow Numpy, Pandas and Keras	Accuracy Cu-DNNLSTM=99.55 Cu-DNNGRU=98.68 Cu-BLSTM=98.90	Full
Alqahtani et al [165]	2022	Real-time dataset	FSO-LSTM GBDT	Normal, DoS DDoS, MIM Spoofing	System equipped with i9 CPU workstation with 16-GB RAM, and 256-GB NVidia Titan Board Python, Keras and OMNET++ used for implementation	Accuracy FSO-LSTM=98.89	9
Pampapathi et al [166]	2022	TON-IoT	FDLNN	Normal, DOS U2R, R2L DoS	-	Accuracy FDLNN=96.12	Full

in Fig. 10. In the confusion matrix, false positives (Type I) and false negatives (Type II) are two types of errors. To improve the model's performance, we need to reduce these errors.

4.4.2 Geometric mean (G-mean)

It offers a balanced assessment, particularly in situations with class imbalance, providing a single measure of overall classification effectiveness. The formula for G-mean is:

$$G - mean = \sqrt{\frac{True\_Pos}{(True\_Pos\ +\ False\_Neg)} * \frac{True\_Neg}{(False\_Pos\ +\ True\_Neg)}}$$

4.4.3 Matthews correlation coefficient (MCC)

It is beneficial for evaluating classification models on imbalanced datasets, providing a comprehensive assessment of their overall performance. The formula for MCC considers all four outcomes of binary classification: true positives (True_pos), true negatives (True_Neg), false positives (False_Pos), and false negatives (False_Neg).

$$MCC = \frac{True\_Pos * True\_Neg - False\_Pos * False\_Neg}{\sqrt{(True\_Pos + False\_Pos)(True\_Pos + False\_Neg)(True\_Neg + False\_Pos)(True\_Neg + False\_Neg)}}$$

4.4.4 Accuracy (Acc)

$$Acc = \frac{True\_Pos\ +\ True\_Neg}{(True\_Pos\ +\ False\_Pos\ +\ True\_Neg\ +\ False\_Neg)}$$

4.4.5 Precision (P_r)

$$P_r = \frac{True\_Pos}{(True\_Pos\ +\ False\_Pos)}$$

4.4.6 True positive rate (TP_r)

$$TP_r = \frac{True\_Pos}{(True\_Pos\ +\ False\_Neg)}$$

4.4.7 False positive rate (FP_r)

$$FP_r = \frac{False\_Pos}{(True\_Neg\ +\ False\_Pos)}$$

Table 11 Detailed analysis of various datasets used to detect DDoS attacks on IoT platforms

Dataset	Year	IoT Traces	Target Classes	Total Features	Benign Flows	Attack Flows	Data Format	Traffic Type
IoTID20 [176]	2020	✓	5	83	40,073	585,710	pcap	Emulated
ToN_IoT [177]	2020	✓	9	46	792,000	21,208,000	pcap, csv	Emulated
IoT-23 [145]	2020	✓	20	21	30,858,735	294,449,255	pcap	Real
MQTT-IoT IDS2020 [178]	2020	✓	5	44	2,843,200	19,938,925	pcap, csv	Emulated
MedBIoT [179]	2020	✓	4	100	12,540,478	5,305,089	pcap	Emulated
IoTNID [180]	2019	✓	5	7	1,756,276	1,229,718	pcap	Emulated
CICDDoS [181]	2019	✗	13	87	56,863	50,006,249	pcap, csv	Emulated
Bot-IoT [154]	2018	✓	11	46	9,543	73,360,900	pcap, csv	Emulated
N-BaIoT [182]	2018	✓	11	115	17,936	831,298	pcap	Real
DS2oS [157]	2018	✓	8	13	347,935	10,017	csv	Emulated
CICIDS [183]	2017	✗	15	79	2,273,097	557,646	pcap, csv	Emulated
UNSW-NB15 [184]	2015	✗	10	49	2,218,761	321,283	pcap, csv	Emulated
ISCX [185]	2012	✗	6	8	2,381,532	68,792	pcap	Emulated
NSL-KDD [186]	2009	✗	5	43	972,781	3,925,650	csv	Emulated

4.4.8 False negative rate (FN_r)

$$FN_r = \frac{False\_Neg}{(True\_Pos + False\_Neg)}$$

4.4.9 True negative rate (TN_r)

$$TN_r = \frac{True\_Neg}{(False\_Pos + True\_Neg)}$$

4.4.10 F-measure (F_m)

$$F_m = 2 * \frac{P_r \ * \ TP_r}{P_r \ + \ TP_r}$$

5 Open research issues and potential solutions

For the IoT domain to continue its rapid growth, there are still some security issues that need to be resolved. As a result of the widespread usage and heterogeneous nature of IoT devices, a single solution is not viable. Therefore, in recent years, several researchers have extensively examined various security mechanisms that address multiple issues related to securing IoT devices. This section presents open issues, significant gaps, and possible solutions that ensure IoT devices' security and prevent them from being exploited to launch large-scale attacks against online infrastructure.

1. **Robust IDS mechanism:** Sometimes, the proposed IDS mechanism itself becomes the victim of an attack while examining the massive volume of network traces [40, 187]. Further, the sophistication in the state-of-art of attacks and attack patterns shifted from Gbps to Tbps due to millions of non-secure devices connected across the globe. Proposed solution: Incremental learning needs to be employed while designing the robust attack detection approach. Data changes continuously in real-world scenarios, but the data used for model designing is completely different from real-world data samples. Therefore, incremental learning is helpful in constantly re-training detection models from real-world traffic. It makes the deployed model more robust and efficient.
2. **Inadequacy of IoT-specific/comprehensive datasets:** IoT devices differ from conventional systems in that they have unique characteristics. Therefore, it requires additional attributes while designing the IDS/DDoS detection model for them. It is essential to design ML and DL-based detection models on an IoT-specific dataset with comprehensive and contemporary attack traffic. Most of the detection mechanisms [127, 128, 130, 132–134, 138, 139] are designed and validated with non-IoT-specific or outdated datasets. These mechanisms failed to provide solutions for modern attacks after deploying the model in today's high-speed and high-volume public networks. Proposed solution: We have characterized several IoT traffic-based datasets in Table 10. Based on the use case, there is a need to select a better dataset for designing the proposed solution. Further, the dataset should have all possible network traffic instances, such as low-rate DDoS, high-rate DDoS traffic, legitimate traffic, flash events, etc.
3. **Unavailability of balanced/preprocessed datasets:** In the detailed analysis of state-of-the-art datasets, we found that most of them are unbalanced. The ML and DL models [117, 135, 136, 147, 149, 153, 157–164, 166] trained with an unbalanced or inappropriate dataset may perform well during training but fail to analyze real-life traffic accurately. The performance of the detection model relies

on the quality of the training data samples. Proposed solution: Synthetic and minority over-sampling techniques (SMOTE), ensembles of datasets, and other dataset-balancing methods can be employed to address this problem. Moreover, different feature-engineering techniques can also be used to prepare a suitable dataset for ML and DL models to improve detection accuracy.

4. **Longer training time of detection model:** Many defense mechanisms [188, 189] face the problem of long training times that affect the model's performance to the point that sometimes it becomes necessary to compromise with the overall performance of the system in order to minimize the training time. The use of DL models is challenging due to the multiple hidden layers involved. Some DL models can be trained in a few weeks or may take several months, increasing the burden and cost of model building and training. Proposed solution: Transfer learning is a method where a pre-trained model is again reused for another problem that belongs to a similar category. Despite its extensive use in different artificial intelligence applications, this concept has not been explored much in cyberattack detection. When ML and DL methods are combined with transfer learning, they improve system performance and achieve better results with less training time.
5. **Validation in simulated environment:** Researchers have designed and validated several defense mechanisms in a simulated or emulated environment. For that purpose, they used simulated datasets for training and evaluating their detection models [125, 143, 144, 148, 150, 151, 162, 166]. However, these datasets do not reflect the actual behavior of real network traffic. As a result, the model performs well in the local environment but fails in the real-life environment. Proposed solution: The proposed model must be developed, validated in a realistic environment, and deployed in the real network for comprehensive evaluation.
6. **Lack of detection models for Zero-day attacks:** The ML-based detection models provided remarkable detection accuracy when the training and validation

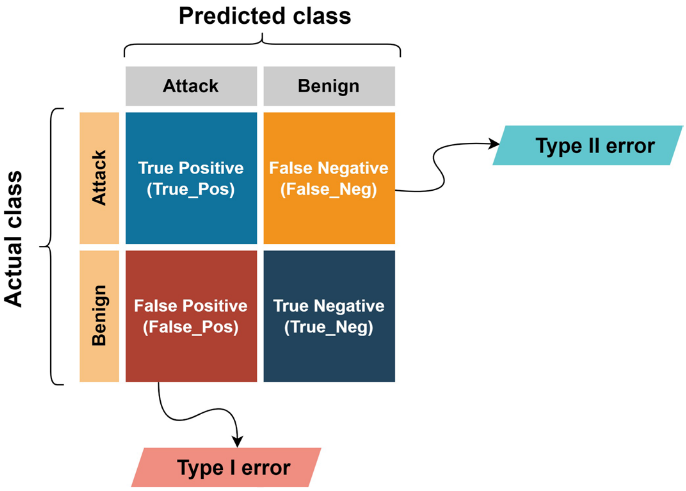

Fig. 10 A confusion matrix

datasets had similar attributes or patterns. However, in reality, attackers typically use different techniques to launch attacks on victims' systems. Therefore, ML-based detection models cannot recognize unseen or zero-day attacks accurately [190, 191]. Proposed solution: A regular update of models is necessary to account for the latest attacks and those that are unknown at training time. Further, select the dataset that contains unknown or zero attacks for the training of the detection models.

7. **Traffic analysis in real time:** A large-scale attack, such as a DDoS attack, overwhelms the target system with numerous bogus requests in a very short time frame. Most detection models in the literature usually operate offline. They are unable to identify patterns that separate benign traffic from malicious traffic and defend against these attacks in an automated way [188, 192]. For DDoS attack detection, analysis of online streaming data hasn't been explored much. Proposed solution: Simplify the analysis process and detect malicious traffic more quickly by reducing the number of network traffic features. Develop high-speed mechanisms to accelerate the traffic analysis process and defend against these attacks in an automated way.
8. **Single-point failure:** Most of the DDoS attack detection approaches [113, 138, 141, 161, 193, 194] are deployed on a centralized architecture. In the event of extensive DDoS attacks, the centralized architecture-based detection approach itself becomes a victim. Further, it failed to analyze large volumes of network traffic packets in real-time. Therefore, these approaches cannot provide comprehensive protection against wide-scale DDoS attacks. Proposed solution: The proposed DDoS attack detection approaches must be deployed on a distributed architecture: Distributed Stream Processing Framework (DSPF). DSPFs, such as Apache Spark Streaming, Apache Kafka Streams, and Apache Storm, are adept at processing large-scale data in a distributed manner, making them valuable tools for analyzing massive network streams.

Practical implications: The reviewed DDoS attack detection approaches have significant and far-reaching implications across various IoT applications, safeguarding critical functionalities and ensuring the reliability of interconnected systems. To highlight the practical implications, we explored specific examples, such as:

- Case 1: e-Healthcare Systems: In scenarios where hospital IoT devices face a DDoS threat, the detection mechanisms quickly identify and counteract attacks, ensuring the seamless operation of life-critical medical devices. Hence, it guarantees uninterrupted patient care and averts potential life-threatening situations.
- Case 2: Smart Industry: In the context of Industrial IoT Networks, DDoS attacks targeting manufacturing IoT devices, the detection methods ensure continuous production line operation by neutralizing DDoS attacks. These methods play a crucial role in maintaining productivity and preventing potential economic losses.
- Case 3: Smart City Infrastructure: A robust protection mechanism can effectively identify and mitigate attacks targeting the city's IoT infrastructure. This

safeguarding secures critical services like traffic management and public safety, ensuring uninterrupted city operations.

- Case 4: Smart Home Networks: Generally, smart home systems are susceptible to DDoS attacks, and practical detection approaches effectively protect against such threats. As a result, it ensures users can continue enjoying automation and security without disruption.

6 Conclusion and future directions

IoT technology has incredible potential to shape a new modern world. It connects everything through the Internet, and we are just one click away from global things. Along with these significant changes that make our day-to-day lives more convenient. However, it also brings several security problems. One of the most prominent security challenge is to protect Internet-based services from large-scale IoT traffic-based DDoS attacks. Therefore, several researchers proposed IoT traffic-based DDoS attack detection approaches in the literature. But, the frequency and magnitude of cyberattacks increase year-after-year.

In this article, we systematically presented: (i) A comprehensive cyberattacks taxonomy for IoT platforms, (ii) Systematically demonstrated IoT's evolution, applications, and challenges, (iii) Discussed various security issues associated with the IoT environment, and demonstrated the review strategy, (iv) Presented a comprehensive review of existing ML and DL-based detection approaches for IoT traffic-based DDoS attacks, (v) Characterized publicly available IoT-traffic-specific datasets with their attributes, and illustrated commonly used performance metrics, (vi) Presented open research issues along with possible solutions for detecting IoT traffic-based DDoS attacks in IoT systems, and future directions. Based on the open issues and their possible solutions, this literature review aims to provide a broader perspective for future directions in the IoT security domain. Therefore, fellow researchers can gain a basic understanding of existing ML and DL-based defense mechanisms for IoT security. Additionally, one can develop a robust defense system to make an IoT environment more secure by addressing the open issues raised in this study.

Declarations

Conflict of interest The authors declare that they have no conflict of interest.

References

1. Chen K, Zhang S, Li Z, Zhang Y, Deng Q, Ray S, Jin Y (2018) Internet-of-things security and vulnerabilities: taxonomy, challenges, and practice. J Hardw Syst Secur 2(2):97–110
2. Vailshery LS (2021) Forecast end-user spending on iot solutions worldwide from 2017 to 2025, https://www.statista.com/statistics/976313/global-iot-market-size/, [Accessed: 2023-01-16]

3. Vailshery L (2022) Number of internet of things (iot) connected devices worldwide from 2019 to 2030, https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/, [Accessed: 2023-01-18]
4. Guan Z, Zhang Y, Wu L, Wu J, Li J, Ma Y, Hu J (2019) Appa: an anonymous and privacy preserving data aggregation scheme for fog-enhanced iot. J Netw Comput Appl 125:82–92
5. Sengupta J, Ruj S, Bit SD (2020) A comprehensive survey on attacks, security issues and blockchain solutions for iot and iiot. J Netw Comput Appl 149:102481
6. Stackup (2020) Timeline - iot history, https://www.stackup.ro/en/2020/12/20/timeline-iot-history/, [Accessed: 2023-01-18]
7. Coding S (2021) Internet of things, https://simplycoding.in/internet-of-things/ , [Accessed: 2023-02-01]
8. IoT S (2020) The rise of iot: The history of the internet of things, https://www.simoniot.com/history-of-iot/, [Accessed: 2023-01-23]
9. Braun A (2019) History of iot: A timeline of development, https://www.iottechtrends.com/history-of-iot/, [Accessed: 2023-01-18]
10. HQSoftware (2018) The history of iot: a comprehensive timeline of major events, infographic, https://hqsoftwarelab.com/blog/the-history-of-iot-a-comprehensive-timeline-of-major-events-infographic/, [Accessed: 2023-01-25]
11. Paul D (2021) Iot devices see more than 1.5bn cyberattacks so far this year, https://www.digit.fyi/iot-security-kaspersky-research-attacks/, [Accessed: 2023-01-25]
12. Tarouco LMR, Bertholdo LM, Granville LZ, Arbiza LMR, Carbone F, Marotta M, De Santanna JJC (2012) Internet of things in healthcare: Interoperatibility and security issues. In: *2012 IEEE International Conference on Communications (ICC)*. IEEE, pp 6121–6125
13. Mohan A (2014) Cyber security for personal medical devices internet of things. In: *2014 IEEE International Conference on Distributed Computing in Sensor Systems*. IEEE, pp 372–374
14. Rahim MA, Rahman MA, Rahman MM, Asyhari AT, Bhuiyan MZA, Ramasamy D (2021) Evolution of iot-enabled connectivity and applications in automotive industry: a review. Vehic Commun 27:100285
15. Hassan R, Qamar F, Hasan MK, Aman AHM, Ahmed AS (2020) Internet of things and its applications: a comprehensive survey. Symmetry 12(10):1674
16. Demestichas K, Peppes N, Alexakis T (2020) Survey on security threats in agricultural iot and smart farming. Sensors 20(22):6458
17. Suryadevara NK, Biswal GR (2019) Smart plugs: Paradigms and applications in the smart city-and-smart grid. Energies 12(10):1957
18. Daia ASA, Ramadan RA, Fayek MB, AETiC A (2018) Sensor networks attacks classifications and mitigation. *Annals of emerging technologies in computing (AETiC), Print ISSN*, pp. 2516–0281
19. Chaudhry J, Saleem K, Haskell-Dowland P, Miraz MH (2018) A survey of distributed certificate authorities in manets. arXiv:1807.03246
20. Bharati TS (2019) Internet of things (iot): a critical review. Int J Sci Technol Res 8(10):227–232
21. Zafeiriou I (2020) Iot and mobility in smart cities. In, 3rd world symposium on communication engineering (WSCE). IEEE 2020:91–95
22. Ryan PJ, Watson RB (2017) Research challenges for the internet of things: what role can or play? Systems 5(1):24
23. Vishwakarma R, Jain AK (2020) A survey of ddos attacking techniques and defence mechanisms in the iot network. Telecommun Syst 73(1):3–25
24. Attia TM (2019) Challenges and opportunities in the future applications of iot technology. International Telecommunications Society (ITS). [Online]. Available: http://hdl.handle.net/10419/201752
25. Ahmad R, Alsmadi I (2021) Machine learning approaches to iot security: a systematic literature review. Int Things 14:100365
26. Imran MA, Zoha A, Zhang L, Abbasi QH (2020) Grand challenges in iot and sensor networks. *Frontiers in communications and networks*, vol. 1. [Online]. Available: https://www.frontiersin.org/article/10.3389/frcmn.2020.619452
27. Al-Hadhrami Y, Hussain FK (2021) Ddos attacks in iot networks: a comprehensive systematic literature review. World Wide Web 24(3):971–1001
28. Chithaluru P, Fadi A-T, Kumar M, Stephan T (2023) “Computational intelligence inspired adaptive opportunistic clustering approach for industrial iot networks,” *IEEE Internet of Things Journal*
29. Banafa A (2017) 3 Major challenges iot is facing. https://www.bbvaopenmind.com/en/technology/digital-world/3-major-challenges-facing-iot/, [Accessed: 2022-03-21]

30. Mishra N, Pandya S (2021) Internet of things applications, security challenges, attacks, intrusion detection, and future visions: a systematic review. IEEE Access 9:59353–59377
31. Kephart JO (2005) Research challenges of autonomic computing. In *Proceedings of the 27th International Conference on Software Engineering*, pp. 15–22
32. Michael R, Daly K (2015) For the internet of things, the cost of cheap will be steep. https://venturebeat.com/2015/01/10/for-the-internet-of-things-the-cost-of-cheap-will-be-steep/, [Accessed: 2023-02-12]
33. Tahsien SM, Karimipour H, Spachos P (2020) Machine learning based solutions for security of internet of things (iot): a survey. J Netw Comput Appl 161:102630
34. Ali ZH, Ali HA, Badawy MM (2015) Internet of things (iot): definitions, challenges and recent research directions. Int J Comput Appl 128(1):37–47
35. Dickson B (2020) Iot botnets might be the cybersecurity industry's next big worry. https://www.iotsecurityfoundation.org/iot-botnets-might-be-the-cybersecurity-industrys-next-big-worry/, [Accessed: 2023-02-12]
36. RAY B (2016) Benefits of quality of service (qos) in lpwan for iot. https://www.link-labs.com/blog/quality-of-service-qos-lpwan-iot#:~:text=Quality%20of%20Service%20(QoS)%20manages,traffic%20and%20registering%20channel%20limits. [Accessed: 2023-02-15]
37. Alansari Z, Anuar NB, Kamsin A, Soomro S, Belgaum MR, Miraz MH, Alshaer J (2018) Challenges of internet of things and big data integration. In: *International Conference for Emerging Technologies in Computing*. Springer, pp. 47–55
38. Cooper J, James A (2009) Challenges for database management in the internet of things. IETE Tech Rev 26(5):320–329
39. Marr B (2018) How much data do we create every day by forbes. https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/?sh=3a88b6f260ba, [Accessed: 2023-02-21]
40. Patil NV, Rama Krishna C, Kumar K (2021) Distributed frameworks for detecting distributed denial of service attacks: a comprehensive review, challenges and future directions,. Concur Computat Pract Exper 33(10):e6197
41. Mittal M, Kumar K, Behal S (2022) Deep learning approaches for detecting ddos attacks: a systematic review. *Soft Computing*, pp 1–37
42. Hossain MM, Fotouhi M, Hasan R (2015) Towards an analysis of security issues, challenges, and open problems in the internet of things. In: ieee world congress on services. IEEE 2015:21–28
43. Elazhary H (2019) Internet of things (iot), mobile cloud, cloudlet, mobile iot, iot cloud, fog, mobile edge, and edge emerging computing paradigms: Disambiguation and research directions. J Netw Comput Appl 128:105–140
44. Zhao K, Ge L (2013) A survey on the internet of things security. Ninth Int Conf Computat Intell Secur 2013:663–667
45. Rashid B, Rehmani MH (2016) Applications of wireless sensor networks for urban areas: a survey. J Netw Comput Appl 60:192–219
46. Touqeer H, Zaman S, Amin R, Hussain M, Al-Turjman F, Bilal M (2021) Smart home security: challenges, issues and solutions at different iot layers. J Supercomput 77(12):14053–14089
47. Atlam HF, Walters R, Wills G (2018) Internet of things: state-of-the-art, challenges, applications, and open issues. Int J Intell Comput Res (IJICR) 9(3):928–938
48. Neely S, Dobson S, Nixon P (2006) Adaptive middleware for autonomic systems. Ann Communi 61(9):1099–1118
49. Razzaque MA, Milojevic-Jevric M, Palade A, Clarke S (2015) Middleware for internet of things: a survey. IEEE Int Things J 3(1):70–95
50. Fortino G, Trunfio P (2014) *Internet of things based on smart objects: Technology, middleware and applications*. Springer
51. Tewari A, Gupta BB (2020) Security, privacy and trust of different layers in internet-of-things (iots) framework. Future Generat Comput Syst 108:909–920
52. Sicari S, Rizzardi A, Grieco LA, Coen-Porisini A (2015) Security, privacy and trust in internet of things: the road ahead. Comput Netw 76:146–164
53. Azrour M, Mabrouki J, Guezzaz A, Kanwal A (2021) Internet of things security: challenges and key issues. Sec Commun Netw 2021:1–11
54. Kumar U, Navaneet S, Kumar N, Pandey SC (2020) Isolation of ddos attack in iot: a new perspective. Wirel Pers Commun 114(3):2493–2510

55. Behal S, Kumar K, Sachdeva M (2018) D-face: an anomaly based distributed approach for early detection of ddos attacks and flash events. J Netw Comput Appl 111:49–63
56. Source W (2021) Ddos attacks. https://www.imperva.com/learn/ddos/ddos-attacks/, [Accessed: 2023-03-09]
57. Nicholson P (2022) Five most famous ddos attacks and then some. https://www.a10networks.com/blog/5-most-famous-ddos-attacks/#:~:text=In%20November%202021%2C%20Microsoft%20mitigated,largest%20DDoS%20attack%20ever%20recorded, [Accessed: 2023-03-12]
58. Cook S (2022) "20+ ddos attack statistics and facts for 2018-2022," https://www.comparitech.com/blog/information-security/ddos-statistics-facts/#:~:text=Research%20shows%20that%20the%20average,2021%20metric%20of%209.15%20Gbps, [Accessed: 2023-03-15]
59. Keshri A (2020) Largest ddos attack ever caught. https://www.getastra.com/blog/knowledge-base/largest-ddos-attack-ever-caught/, [Accessed: 2023-03-10]
60. MacKay J (2019) Largest ddos attack ever caught10 biggest ddos attacks and how your organisation can learn from them. https://www.metacompliance.com/blog/10-biggest-ddos-attacks-and-how-your-organisation-can-learn-from-them/, [Accessed: 2023-03-10]
61. Warburton D (2022) 2022 application protection report: Ddos attack trends. https://www.f5.com/labs/articles/threat-intelligence/2022-application-protection-report-ddos-attack-trends, [Accessed: 2023-03-15]
62. Stahie S (2022) Google mitigates largest ddos attack in its history. https://www.bitdefender.com/blog/hotforsecurity/google-mitigates-largest-ddos-attack-in-its-history/, [Accessed: 2023-11-15]
63. Thakkar J (2020) 20+ ddos attack statistics and facts for 2018-2022. https://sectigostore.com/blog/ddos-attack-statistics-a-look-at-the-most-recent-and-largest-ddos-attacks/, [Accessed: 2023-02-23]
64. Crowdstrike (2022) What is a botnet? https://www.crowdstrike.com/cybersecurity-101/botnets/, [Accessed: 2023-03-15]
65. Doshi K, Yilmaz Y, Uludag S (2021) Timely detection and mitigation of stealthy ddos attacks via iot networks. IEEE Trans Depend Secure Comput 18(5):2164–2176
66. Perrone G, Vecchio M, Pecori R, Giaffreda R *et al.* (2017) The day after mirai: A survey on mqtt security solutions after the largest cyber-attack carried out through an army of iot devices. In *IoT-BDS*, pp. 246–253
67. Haddud A, DeSouza A, Khare A, Lee H (2017) Examining potential benefits and challenges associated with the internet of things integration in supply chains. *J Manuf Technol Manag*
68. Salim MM, Rathore S, Park JH (2020) Distributed denial of service attacks and its defenses in iot: a survey. J Supercomput 76(7):5320–5363
69. Kleberger P, Olovsson T, Jonsson E (2011) Security aspects of the in-vehicle network in the connected car. In (2011) IEEE Intelligent Vehicles Symposium (IV). IEEE 528–533
70. Mathonsi T, Tshilongamulenzhe T, Buthelezi B (2019) Blockchain security model for internet of things. In *The Proceedings of Academics World 158th International Conference*, pp. 52–56
71. Ram P, Markkula J, Friman V, Raz A (2018) Security and privacy concerns in connected cars: a systematic mapping study. In: *2018 44th Euromicro Conference on Software Engineering and Advanced Applications (SEAA)*. IEEE, pp. 124–131
72. Shepherd A, Kesa C, Cooper J (2020) Internet of things (iot) medical security: taxonomy and perception. Issues Information Syst 21:3
73. Sethi P, Sarangi SR (2017) Internet of things: architectures, protocols, and applications. J Electr Comput Eng 26:2017
74. Asghari P, Rahmani AM, Javadi HHS (2018) Service composition approaches in iot: a systematic review. J Netw Comput Appl 120:61–77
75. Zheng L, Zhang H, Han W, Zhou X, He J, Zhang Z, Gu Y, Wang J et al (2011) Technologies, applications, and governance in the internet of things. Internet of things-Global technological and societal trends, From smart environments and spaces to green ICT
76. Fadele AA, Othman M, Hashem IAT, Yaqoob I, Imran M, Shoaib M (2019) A novel countermeasure technique for reactive jamming attack in internet of things. Multim Tools Appl 78(21):29899–29920
77. Jan MA, Khan M (2013) Denial of service attacks and their countermeasures in wsn. IRACST-Int J Comput Netw Wirel Commun (IJCNWC) 3:1–6
78. Wang Y, Attebury G, Ramamurthy B (2006) A survey of security issues in wireless sensor networks

79. Borgohain T, Kumar U, Sanyal S (2015) Survey of security and privacy issues of internet of things. *arXiv preprint*arXiv:1501.02211
80. Bhattasali T, Chaki R, Sanyal S (2012) Sleep deprivation attack detection in wireless sensor network. *arXiv preprint*arXiv:1203.0231
81. Bhunia S, Tehranipoor M (2019) Chapter 8 - side-channel attacks. In *Hardware Security*, S. Bhunia and M. Tehranipoor, Eds. Morgan Kaufmann, pp. 193–218. [Online]. Available: https://www.sciencedirect.com/science/article/pii/B9780128124772000137
82. OS JN, Bhanu SMS (2018) "A survey on code injection attacks in mobile cloud computing environment," in *2018 8th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*. IEEE, pp. 1–6
83. Adefemi Alimi KO, Ouahada K, Abu-Mahfouz AM, Rimer S (2020) A survey on the security of low power wide area networks: Threats, challenges, and potential solutions. Sensors 20(20):5800
84. Mosenia A, Jha NK (2016) A comprehensive study of security of internet-of-things. IEEE Trans emerg topics comput 5(4):586–602
85. Specht SM, Lee RB (2003) Distributed denial of service: taxonomies of attacks, tools and countermeasures, princeton architecture laboratory for multimedia and security. ISCA, Princeton, NJ
86. Yaar A, Perrig A, Song D, "Siff: A stateless internet flow filter to mitigate ddos flooding attacks," in IEEE Symposium on Security and Privacy, (2004) Proceedings. 2004. IEEE 2004:130–143
87. Chapade S, Pandey K, Bhade D (2013) "Securing cloud servers against flooding based ddos attacks. In: *2013 International Conference on Communication Systems and Network Technologies*. IEEE, pp. 524–528
88. Srivastava A, Gupta B, Tyagi A, Sharma A, Mishra A (2011) A recent survey on ddos attacks and defense mechanisms. In *International Conference on Parallel Distributed Computing Technologies and Applications*. Springer, pp. 570–580
89. Alomari E, Manickam S, Gupta BB, Karuppayah S, Alfaris R (2012) Botnet-based distributed denial of service (ddos) attacks on web servers: classification and art. *arXiv preprint*arXiv:1208.0403*,*
90. Lemon J (2002) Resisting {SYN} flood {DoS} attacks with a {SYN} cache. In *BSDCon 2002 (BSDCon 2002)*
91. Lee RB (2004) Taxonomies of distributed denial of service networks, attacks, tools, and countermeasures. *Princeton University*
92. Yan Q, Huang W, Luo X, Gong Q, Yu FR (2018) A multi-level ddos mitigation framework for the industrial internet of things. IEEE Commun Magaz 56(2):30–36
93. Phan TV, Bao NK, Park M (2016) "A novel hybrid flow-based handler with ddos attacks in software-defined networking. In: (2016) Intl IEEE Conferences on Ubiquitous Intelligence & Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld). IEEE 350–357
94. Nagy B, Orosz P, Tóthfalusi T, Kovács L, Varga P (2018) "Detecting ddos attacks within milliseconds by using fpga-based hardware acceleration," in *NOMS 2018-2018 IEEE/IFIP Network Operations and Management Symposium*. IEEE, pp. 1–4
95. Wankhede SB (2019) Study of network-based dos attacks. In: *Nanoelectronics, circuits and communication systems*. Springer, pp. 611–616
96. Patel J, Katkar V (2016) A multi-classifiers based novel dos/ddos attack detection using fuzzy logic. In: *proceedings of International Conference on ict for Sustainable Development*. Springer, pp. 809–815
97. Kührer M, Hupperich T, Rossow C, Holz T (2014) "Exit from hell? reducing the impact of {Amplification}{DDoS} attacks," in *23rd USENIX Security Symposium (USENIX Security 14)*, pp. 111–125
98. Kawamura T, Fukushi M, Hirano Y, Fujita Y, Hamamoto Y (2017) "An ntp-based detection module for ddos attacks on iot. In: *2017 IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW)*. IEEE, pp. 15–16
99. Hoque N, Bhattacharyya DK, Kalita JK (2015) Botnet in ddos attacks: trends and challenges. IEEE Commun Surv Tutor 17(4):2242–2270
100. Elleithy KM, Blagovic D, Cheng WK, Sideleau P (2005) Denial of service attack techniques: analysis, implementation and comparison
101. Acharya AA, Arpitha K, Kumar B (2016) An intrusion detection system against udp flood attack and ping of death attack (ddos) in manet. Int J Eng Technol (IJET) 8:2

102. Bhuyan MH, Bhattacharyya D, Kalita JK (2015) An empirical evaluation of information metrics for low-rate and high-rate ddos attack detection. Patt Recogn Lett 51:1–7
103. Gupta N, Jain A, Saini P, Gupta V (2016) Ddos attack algorithm using icmp flood. In: *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)*. IEEE, pp. 4082–4084
104. Mohammadi R, Javidan R, Conti M (2017) Slicots: An sdn-based lightweight countermeasure for tcp syn flooding attacks. IEEE Trans Netw Serv Manag 14(2):487–497
105. Valarmathi M, Meenakowshalya A, Bharathi A (2016) Robust sybil attack detection mechanism for social networks-a survey. In: (2016) 3rd International Conference on Advanced Computing and Communication Systems (ICACCS), vol. 1. IEEE 1–5
106. Evangelista D, Mezghani F, Nogueira M, Santos A, Evaluation of sybil attack detection approaches in the internet of things content dissemination. In: (2016) Wireless Days (WD). IEEE 2016:1–6
107. Mathew A, Terence JS (2017) A survey on various detection techniques of sinkhole attacks in wsn. In: *2017 International Conference on Communication and Signal Processing (ICCSP)*. IEEE, pp. 1115–1119
108. Mirkovic J, Reiher P (2004) A taxonomy of ddos attack and ddos defense mechanisms. ACM SIGCOMM Comput Commun Rev 34(2):39–53
109. Cambiaso E, Papaleo G, Aiello M (2012) Taxonomy of slow dos attacks to web applications. In: *International Conference on Security in Computer Networks and Distributed Systems*. Springer, pp. 195–204
110. Damon E, Dale J, Laron E, Mache J, Land N, Weiss R (2012) Hands-on denial of service lab exercises using slowloris and rudy. In: *Proceedings of the 2012 Information Security Curriculum Development Conference*, pp. 21–29
111. Kambourakis G, Moschos T, Geneiatakis D, Gritzalis S (2007) Detecting dns amplification attacks. In *International workshop on critical information infrastructures security*. Springer, pp. 185–196
112. Ehlert S, Geneiatakis D, Magedanz T (2010) Survey of network security systems to counter sip-based denial-of-service attacks. Comput Sec 29(2):225–243
113. Soe YN, Feng Y, Santosa PI, Hartanto R, Sakurai K (2020) Machine learning-based iot-botnet attack detection with sequential architecture. Sensors 20(16):4372
114. Lawal MA, Shaikh RA, Hassan SR (2021) A ddos attack mitigation framework for iot networks using fog computing. Procedia Comput Sci 182:13–20
115. Shafiq M, Tian Z, Bashir AK, Du X, Guizani M (2020) Corrauc: a malicious bot-iot traffic detection method in iot network using machine-learning techniques. IEEE Int Things J 8(5):3242–3254
116. Doshi R, Apthorpe N, Feamster N (2018) Machine learning ddos detection for consumer internet of things devices. In: (2018) IEEE security and privacy workshops (SPW). IEEE 29–35
117. Churcher A, Ullah R, Ahmad J, Ur Rehman S, Masood F, Gogate M, Alqahtani F, Nour B, Buchanan WJ (2021) An experimental analysis of attack classification using machine learning in iot networks. Sensors 21(2):446
118. Aysa MH, Ibrahim AA, Mohammed AH (2020) Iot ddos attack detection using machine learning. In: (2020) 4th international symposium on multidisciplinary studies and innovative technologies (ISMSIT). IEEE 1–7
119. Ullah I, Mahmoud QH (2020) A technique for generating a botnet dataset for anomalous activity detection in iot networks. In *2020 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*. IEEE, pp. 134–140
120. Samdekar R, Ghosh S, Srinivas K (2021) Efficiency enhancement of intrusion detection in iot based on machine learning through bioinspire. In *2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV)*. IEEE, pp. 383–387
121. Pokhrel S, Abbas R, Aryal B (2021) Iot security: botnet detection in iot using machine learning. *arXiv preprint*arXiv:2104.02231
122. Seifousadati A, Ghasemshirazi S, Fathian M (2021) A machine learning approach for ddos detection on iot devices. *arXiv preprint*arXiv:2110.14911
123. Nimbalkar P, Kshirsagar D (2021) Feature selection for intrusion detection system in internet-of-things (iot). ICT Express 7(2):177–181
124. Das A, Sunitha B et al (2022) An efficient feature selection approach for intrusion detection system using decision tree. Int J Adv Comput Sci Appl 13:2
125. Alduailij M, Khan QW, Tahir M, Sardaraz M, Alduailij M, Malik F (2022) Machine-learning-based ddos attack detection using mutual information and random forest feature importance method. Symmetry 14(6):1095

126. Shukla P, Krishna CR, Patil NV (2023) Eiot-ddos: embedded classification approach for iot traffic-based ddos attacks. *Cluster Computing*, pp. 1–20
127. Dwivedi S, Vardhan M, Tripathi S (2020) Distributed denial-of-service prediction on iot framework by learning techniques. Open Comput Sci 10(1):220–230
128. Rani D, Kaushal NC (2020) Supervised machine learning based network intrusion detection system for internet of things. In: *2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*. IEEE, pp. 1–7
129. Chen Y-W, Sheu J-P, Kuo Y-C, Van Cuong N (2020) Design and implementation of iot ddos attacks detection system based on machine learning. In: *2020 European Conference on Networks and Communications (EuCNC)*. IEEE, pp. 122–127
130. Chesney S, Roy K, Khorsandroo S (2020) Machine learning algorithms for preventing iot cybersecurity attacks. In: *proceedings of SAI Intelligent Systems Conference*. Springer, pp. 679–686
131. Syed NF, Baig Z, Ibrahim A, Valli C (2020) Denial of service attack detection through machine learning for the iot. J Inform Telecommun 4(4):482–503
132. Ahmad M, Riaz Q, Zeeshan M, Tahir H, Haider SA, Khan MS (2021) Intrusion detection in internet of things using supervised machine learning based on application and transport layer features using unsw-nb15 data-set. EURASIP J Wirel Commun Netw 2021(1):1–23
133. Alzahrani RJ, Alzahrani A (2021) Security analysis of ddos attacks using machine learning algorithms in networks traffic. Electronics 10(23):2919
134. Anwer M, Khan S, Farooq M et al (2021) Attack detection in iot using machine learning. Eng Technol Appl Sci Res 11(3):7273–7278
135. Krishnan S, Neyaz A, Liu Q (2021) Iot network attack detection using supervised machine learning. Int J Artif Intell Expert Syst 10:18–32
136. Kumar P, Bagga H, Netam BS, Uduthalapally V (2022) Sad-iot: Security analysis of ddos attacks in iot networks. Wirel Pers Commun 122(1):87–108
137. Saghezchi FB, Mantas G, Violas MA, de Oliveira Duarte AM, Rodriguez J (2022) Machine learning for ddos attack detection in industry 4.0 cppss. Electronics 11(4):602
138. Gaur V, Kumar R (2022) Analysis of machine learning classifiers for early detection of ddos attacks on iot devices. Arabian J Sci Eng 47(2):1353–1374
139. Amrish R, Bavapriyan K, Gopinaath V, Jawahar A, Kumar CV (2022) Ddos detection using machine learning techniques. J IoT Soc Mob Anal Cloud 4(1):24–32
140. Larriva-Novo X, Villagrá VA, Vega-Barbas M, Rivera D, Sanz Rodrigo M (2021) An iot-focused intrusion detection system approach based on preprocessing characterization for cybersecurity datasets. Sensors 21(2):656
141. Popoola SI, Adebisi B, Ande R, Hammoudeh M, Anoh K, Atayero AA (2021) smote-drnn: a deep learning algorithm for botnet detection in the internet-of-things networks. Sensors 21(9):2985
142. Dutta V, Choras M, Pawlicki M, Kozik R (2020) Detection of cyberattacks traces in iot data. J Univers Comput Sci 26(11):1422–1434
143. Roopak M, Tian GY, Chambers J (2020) An intrusion detection system against ddos attacks in iot networks. In: (2020) 10th Annual Computing and Communication Workshop and Conference (CCWC). IEEE pp 0562–0567
144. Meidan Y, Sachidananda V, Peng H, Sagron R, Elovici Y, Shabtai A (2020) A novel approach for detecting vulnerable iot devices connected behind a home nat. Comput Sec 97:101968
145. Dutta V, Choraś M, Pawlicki M, Kozik R (2020) A deep learning ensemble for network anomaly and cyber-attack detection. Sensors 20(16):4583
146. Haq MA, Khan MAR (2022) Dnnbot: deep neural network-based botnet detection and classification. CMC-Comput Mater Cont 71(1):1729–1750
147. Ahmad Z, Shahid Khan A, Nisar K, Haider I, Hassan R, Haque MR, Tarmizi S, Rodrigues JJ (2021) Anomaly detection using deep neural network for iot architecture. Appl Sci 11(15):7050
148. Sharma DK, Dhankhar T, Agrawal G, Singh SK, Gupta D, Nebhen J, Razzak I (2021) Anomaly detection framework to prevent ddos attack in fog empowered iot networks. Ad Hoc Netw 121:102603
149. Zeeshan M, Riaz Q, Bilal MA, Shahzad MK, Jabeen H, Haider SA, Rahim A (2021) Protocol-based deep intrusion detection for dos and ddos attacks using unsw-nb15 and bot-iot data-sets. IEEE Access 10:2269–2283
150. Wazzan M, Algazzawi D, Albeshri A, Hasan S, Rabie O, Asghar MZ (2022) Cross deep learning method for effectively detecting the propagation of iot botnet. Sensors 22(10):3895

151. Shahhosseini M, Mashayekhi H, Rezvani M (2022) A deep learning approach for botnet detection using raw network traffic data. J Netw Syst Manag 30(3):1–23
152. Chaudhary P, Gupta B, Singh A (2022) Implementing attack detection system using filter-based feature selection methods for fog-enabled iot networks. *Telecommun Syst*, pp 1–17
153. Hezam AA, Mostafa SA, Baharum Z, Alanda A, Salikon MZ (2021) Combining deep learning models for enhancing the detection of botnet attacks in multiple sensors internet of things networks,. JOIV: Int J Inform Visualiz 5(4):380–387
154. Koroniotis N, Moustafa N, Sitnikova E, Turnbull B (2019) Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: bot-iot dataset. Future Gener Comput Syst 100:779–796
155. Kim J, Shin N, Jo SY, Kim SH (2017) Method of intrusion detection using deep neural network. In: (2017) IEEE International Conference on Big Data and Smart Computing (BigComp). IEEE 313–316
156. Feng F, Liu X, Yong B, Zhou R, Zhou Q (2019) Anomaly detection in ad-hoc networks based on deep learning model: a plug and play device. Ad Hoc Netw 84:82–89
157. Latif S, Zou Z, Idrees Z, Ahmad J (2020) A novel attack detection scheme for the industrial internet of things using a lightweight random neural network. IEEE Access 8:89337–89350
158. Badamasi UM, Khaliq S, Babalola O, Musa S, Iqbal T (2020) A deep learning based approach for ddos attack detection in iot-enabled smart environments. Int J Comput Netw Commun Secu 8(10):93–99
159. Alkahtani H, Aldhyani TH (2021) Botnet attack detection by using cnn-lstm model for internet of things applications. *Security and Communication Networks*, 2021
160. Ge M, Syed NF, Fu X, Baig Z, Robles-Kelly A (2021) Towards a deep learning-driven intrusion detection approach for internet of things. Comput Netw 186:107784
161. Apostol I, Preda M, Nila C, Bica I (2021) Iot botnet anomaly detection using unsupervised deep learning. Electronics 10(16):1876
162. Cil AE, Yildiz K, Buldu A (2021) Detection of ddos attacks with feed forward based deep neural network model. Expert Syst Appl 169:114520
163. Nasir M, Javed AR, Tariq MA, Asim M, Baker T (2022) Feature engineering and deep learning-based intrusion detection framework for securing edge iot. J Supercomput 78(6):8852–8866
164. Al Razib M, Javeed D, Khan MT, Alkanhel R, Muthanna MSA (2022) Cyber threats detection in smart environments using sdn-enabled dnn-lstm hybrid framework. IEEE Access 10:53 015-53 026
165. Alqahtani AS (2022) Fso-lstm ids: hybrid optimized and ensembled deep-learning network-based intrusion detection system for smart networks. J Supercomput 78(7):9438–9455
166. Pampapathi B, Guptha N, Hema M (2022) Towards an effective deep learning-based intrusion detection system in the internet of things. Telemat Inform Rep 7:100009
167. Abdulsahib GM, Selvaraj DS, Manikandan A, Palanisamy S, Uddin M, Khalaf OI, Abdelhaq M, Alsaqour R (2023) Reverse polarity optical orthogonal frequency division multiplexing for high-speed visible light communications system. Egypt Inform J 24(4):100407
168. Xue X, Abdulsahib GM, Khalaf OI, Jagan J, Loganathan K, Makota C, Ponraj B (2023) Soft computing approach on estimating the lateral confinement coefficient of cfrp veiled circular columns. Alexand Eng J 81:599–619
169. Homod RZ, Mohammed HI, Abderrahmane A, Alawi OA, Khalaf OI, Mahdi JM, Guedri K, Dhaidan NS, Albahri A, Sadeq AM et al (2023) Deep clustering of lagrangian trajectory for multi-task learning to energy saving in intelligent buildings using cooperative multi-agent. Appl Energy 351:121843
170. Xue X, Palanisamy S, Manikandan A, Selvaraj D, Khalaf OI, Abdulsahib GM (2023) A novel partial sequence technique based chaotic biogeography optimization for papr reduction in generalized frequency division multiplexing waveform. Heliyon 9:9
171. Rana SK, Rana AK, Rana SK, Sharma V, Lilhore UK, Khalaf OI, Galletta A (2023) Decentralized model to protect digital evidence via smart contracts using layer 2 polygon blockchain. *IEEE Access*
172. Khalaf OISRA, Dhanasekaran S, Abdulsahib GM et al (2023) A decision science approach using hybrid eeg feature extraction and gan-based emotion classification. Adv Decis Sci 27(1):172–191
173. Chang BH, Channa KA, Uche E, Khalaf OI, Ali OW (2022) Analyzing the impacts of terrorism on innovation activity: a cross country empirical study. Adv Decis Sci 26:124–161
174. Tang Z, Xie H, Du C, Liu Y, Khalaf OI, Allimuthu UK (2022) Machine learning assisted energy optimization in smart grid for smart city applications. J Interconnec Netw 22(Supp03):2144006

175. Goswami S, Sagar AK, Nand P, Khalaf OI (2022) Time series analysis using stacked lstm model for indian stock market. In: *2022 IEEE IAS Global Conference on Emerging Technologies (GlobConET)*. IEEE, pp. 399–405
176. Ullah I, Mahmoud QH (2020) A scheme for generating a dataset for anomalous activity detection in iot networks. In: *Canadian Conference on Artificial Intelligence*. Springer, pp. 508–520
177. Booij TM, Chiscop I, Meeuwissen E, Moustafa N, den Hartog FT (2021) Ton_iot: the role of heterogeneity and the need for standardization of features and attack types in iot network intrusion data sets. IEEE Int Things J 9(1):485–496
178. Hindy H, Bayne E, Bures M, Atkinson R, Tachtatzis C, Bellekens X (2020) Machine learning based iot intrusion detection system: an mqtt case study (mqtt-iot-ids2020 dataset). In: *International Networking Conference*. Springer, pp. 73–84
179. Guerra-Manzanares A, Medina-Galindo J, Bahsi H, Nõmm S (2020) Medbiot: generation of an iot botnet dataset in a medium-sized iot network. In *ICISSP*, pp. 207–218
180. Liu Z, Thapa N, Shaver A, Roy K, Yuan X, Khorsandroo S (2020) Anomaly detection on iot network intrusion using machine learning. In: (2020) International Conference on Artificial Intelligence, Big Data, Computing and Data Communication Systems (icABCD). IEEE 1–5
181. Cic ddos dataset (2019) https://www.unb.ca/cic/datasets/ddos-2019.html, [Accessed: 2022-11-27]
182. Meidan Y, Bohadana M, Mathov Y, Mirsky Y, Shabtai A, Breitenbacher D, Elovici Y (2018) N-baiot: network-based detection of iot botnet attacks using deep autoencoders. IEEE Pervas Comput 17(3):12–22
183. Cicids dataset (2017) https://www.unb.ca/cic/datasets/ids-2017.html, [Accessed: 2022-11-27]
184. Moustafa N, Slay J (2015) Unsw-nb15: a comprehensive data set for network intrusion detection systems (unsw-nb15 network data set). In: (2015) Military Communications and Information Systems Conference (MilCIS). IEEE 1–6
185. Iscx-2012 dataset (2012) https://www.unb.ca/cic/datasets/ids.html, [Accessed: 2022-11-28]
186. Nsl-kdd dataset (2009) https://www.unb.ca/cic/datasets/nsl.html, [Accessed: 2022-11-28]
187. Khraisat A, Alazab A (2021) A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges. Cybersecurity 4:1–27
188. Bhayo J, Jafaq R, Ahmed A, Hameed S, Shah SA (2021) A time-efficient approach toward ddos attack detection in iot network using sdn. IEEE Int Things J 9(5):3612–3630
189. Lutsiv N, Maksymyuk T, Beshley M, Lavriv O, Andrushchak V, Sachenko A, Vokorokos L, Gazda J (2022) Deep semisupervised learning-based network anomaly detection in heterogeneous information systems. Comput Mater Cont 70:1
190. Yilmaz Y, Buyrukoğlu S (2022) Development and evaluation of ensemble learning models for detection of ddos attacks in iot. Hittite J Sci Eng 9(2):73–82
191. Yilmaz Y, Halak B (2019) A two-flights mutual authentication for energy-constrained iot devices. In: (2019) IEEE 4th international verification and security workshop (IVSW). IEEE 31–36
192. Santhosh Kumar S, Selvi M, Kannan A *et al.* (2023) A comprehensive survey on machine learning-based intrusion detection systems for secure communication in internet of things. *Computational intelligence and neuroscience*, 2023
193. Gupta B, Chaudhary P, Chang X, Nedjah N (2022) Smart defense against distributed denial of service attack in iot networks using supervised learning classifiers. Comput Electr Eng 98:107726
194. Adefemi Alimi KO, Ouahada K, Abu-Mahfouz AM, Rimer S, Alimi OA (2022) Refined lstm based intrusion detection for denial-of-service attack in internet of things. J Sens Actuat Netw 11(3):32

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.