Cyber Security and Applications 3 (2025) 100085

Contents lists available at ScienceDirect

Cyber Security and Applications

journal homepage: http://www.keaipublishing.com/en/journals/cyber-security-and-applications/

Deep learning-driven defense strategies for mitigating DDoS attacks in cloud computing environments

Doaa Mohsin Abd Ali Afraji[a,b], Jaime Lloret[a,*], Lourdes Peñalver[c]

[a] Department of Computer Engineering, Universitat Politècnica de València, Valencia, Spain
[b] Department of Computer Science, College of Education, Mustansiriyah University, Baghdad, Iraq
[c] Integrated Management Coastal Zones Research Institute, Universitat Politècnica de València, Valencia, Spain

ARTICLE INFO

Keywords:
DDoS attacks
Internet of things
Deep learning
Cybersecurity
Explainable AI
Dataset limitations
Machine learning algorithms

ABSTRACT

The kind of cyber threat prevalent and most dangerous to networked systems is the Distributed Denial of Service (DDoS), especially with expanded connection of Internet of Things (IoT) devices. This article categorizes DDoS attacks into three primary types: volumetric, protocol based and application layer of cyber attacks. It discusses the application of security threats that arise from the use of the DL models, accusing recently introduced ideas and stressing pitfalls: the issues of data and methods scarcity. There is the same need for the greater use of explainable and transparent AI to improve confidence in such security systems as is noted in the review. It also reveals that present detection performance is constrained and frequently obstructed by the poor quality of the datasets. The future work is proposed to build superior datasets and use accurate algorithm to improve the security models. This paper focuses on explainability as a way of making the AI model creation process and any consequent decisions explainable and transparent. The use of deep learning enhances the capability of cybersecurity in handling DDoS attacks and preventing or controlling them. But it has to be a part of a more large-scope platform, based on multiple types of longitudinal or cross-sectional data combined with high efficiency, explainable AI. The article ends with call to proceed with studying and advancing the AI application in response to new threats, and make the most of it to enhance protection of the contemporary networked environment.

1. Introduction

Cloud computing forms the backbone of modern digital infrastructure, offering more agile and cost-effective solutions. These services enable organizations to optimize operations and scale resources according to demand, making advanced computing accessible to a broader range of users [1]. The shift from traditional computing, with its high overhead and maintenance costs, has transformed the landscape, allowing smaller enterprises to participate in technology-driven markets [2].

One of the key points which affects this very layer and has a broad impact in terms of IT spend is cost economics (of cloud computing) especially when it comes to infrastructure management as one area. This can enable demand-based resource allocation, reducing the risk of over- or under-provisioning. This approach is designed to foster IT resource management at a pace that better aligns consumer behavior with operational needs, which in turn means more sustainable IT consumption [3]. That said, security issues including default key breaches and large-scale unauthorized access reinforce the importance of implementing cloud threat prevention technology. This is imperative to ensure data protection for sensitive data and to uphold the trust that cloud service providers hold with their existing or potential customers [4]. Cloud services are threatened by Distributed Denial of Service (DDoS) attacks that need some intelligent security mechanisms to detect and respond for it's persistently nature otherwise they can disrupt the service delivery from Cloud provider [5]. However, cloud computing has changed the scalability and operational efficiency but security risks coming from it need to be circumvented for continued development and stability. The entire digital economy relies on cloud and its continuous evolution towards a more secure platform should be of highest priority. DDoS attacks continue to be a significant threat in the computer security context, disrupting services by saturating a network with more traffic than it can efficiently handle or that is required for normal operation and thereby causing the network to become unavailable to any of its intended users [1,6]. This methodology is based on the use of botnets, with networks composed of infected devices which send a high volume amount of traffic to target systems to disrupt its availability [7]. Amplification and reflection are some common techniques to increase the volume of traffic, which will heavily endanger the integrity of network services [3].

Peer review under responsibility of KeAi Communications Co., Ltd.
* Corresponding author.
E-mail addresses: jlloret@dcom.upv.es (J. Lloret), lourdes@disca.upv.es (L. Peñalver).

https://doi.org/10.1016/j.csa.2025.100085
Received 1 September 2024; Received in revised form 7 November 2024; Accepted 8 January 2025
Available online 10 January 2025

The cloud environment might be more vulnerable to DDoS attacks, for example due to attackers using compromised systems as reflectors or ampliers with the potential of creating huge trac oods, interfering service continuity and reliability [8]. Defense everywhere must differentiate between legit and malicious packets. Moreover, anomaly-based systems are capable of detecting unknown attack vectors even zero-day threats by identifying deviations from expected traffic behaviour [2], whereas, signature-based defense techniques utilize predefined patterns to identify attack known threats. DL: Deep Learning is a great suite to identify malicious traffic within the networks. Modern DL-based algorithms can learn complex patterns from basic traffic data and achieve effective separation of DDoS traffic [9]. Apart from DDoS attack protection, these models are used in multiple aspects of cybersecurity namely cloud data encryption, malware detection and secure data transfer to name a few. DL can model complex, nonlinear and hierarchical features thus can suit the solution for cybersecurity issues at both low-level abstractions [4].

The complexity of cloud-based DDoS attacks requires robust, adaptable defenses. DL provides dynamic cybersecurity solutions for these increasingly sophisticated threats. As DDoS attacks become more frequent and diverse, DL-based methods offer promising solutions for detecting and neutralizing them. However, continuous innovation is necessary to maintain the effectiveness of cloud service defenses. Deep Neural Networks (DNNs), which form the basis of DL, consist of multiple processing layers that perform nonlinear transformations to detect cyber threats. This architecture, commonly used in fields like image recognition, is adept at detecting subtle changes in attack patterns, a capability crucial for identifying DDoS attempts. In fact, DL models have achieved accuracy rates exceeding 99% in certain scenarios [10]. Recent advancements, such as Unsupervised Stacked Autoencoders (SAs) combined with Decision Trees (DTs), have proven effective in handling unbalanced datasets, enhancing the detection of cyber threats [11].

However, despite its advantages, using DL to detect web-based attacks presents challenges. For instance, distinguishing between benign and malicious URLs remains difficult due to the diverse nature of web traffic. Developing systems capable of converting different URL types into formats suitable for DL models, as well as identifying new attack signatures, requires further research [12]. Deploying DL to mitigate DDoS attacks in cloud environments holds great potential but involves significant challenges. Cloud infrastructures are particularly vulnerable to such attacks, and while DL offers solutions for detecting complex attack patterns, the industry faces obstacles such as a lack of comprehensive cloud-specific DDoS datasets and the need for AI models that are both transparent and explainable. Technological advancements, alongside a shift towards accountable AI systems, will be essential for strengthening cloud-based defenses against sophisticated cyberattacks.

2. Deep learning application in DDoS

2.1. Distributed denial of service attacks

DDoS attacks use botnets of millions of compromised machines to overwork IoT networks with more traffic than the network can handle, as a result failing and interrupting services. They deplete system resources, disable network infrastructure, halt service operations and interfere with users from accessing online services. Typically, reflection and amplification methods are used in these attacks. With reflection attacks, a target is confused as to what IP the network communication originated from and is targeted by traffic from multiple endpoints. In contrast, amplification attacks create a high amount of traffic by sending a large number of packets to the target system [13].

Unfortunately, these are just a handful of DDoS attack types. Based on its interface (Command Line Interface vs. Graphical User Interface), Fig. 1 also shows a classification of the major types of DDoS attacks according to the dynamics in which are carried out (continuous, variable, increasing or fluctuating) and their overall targets (resource depletion, bandwidth depletion and a mixture of both), as well as whether it is directed at leaving offline a network link or an endpoint. These categories allow a better view on how these attacks work within networks, propitiating a more organized way to understand the mitigation of such types of threats.

This categorization helps to illustrate these pervasive, polymorphic behavior DDoS attacks, indicating the need for layered defense schemes. As we dissect these attacks, it is obvious that security frameworks will require a new level of progression to protect IoT networks successfully, from the more complex and changing strategies of DDoS campaigns. This calls for a comprehensive cybersecurity functionality, where systems respond to potential threats, as well as run preemptively to neutralize them. From the current trends, it is apparent that an IoT network with such a multi layer defense system (utilizes existing security protocols and applies advanced DL algorithms) is able to withstand the growing number of threats posed by DDoS. This can result in more intelligent and responsive IoT security solutions which are robust against cutting edge DDoS tactics designed to probe modern day network infrastructures. If the DDoS attack tools are considered in depth, the first aspect to note is whether they precedence in protocol based attacks or in application based attacks, both of which are quite versatile attacks but living in different network layers. By all means, protocol based cyberattacks make the most of efforts only to exhaust the servers that support them and hinder the intermediaries of server client communication such as firewalls and load balancers. They also are performed by bombarding the server with an excessive count of false protocol requests, which results in the clogging of server resources. These attacks are measured at a critical rate in packets per second (pps) and target network layer protocol vulnerabilities in order to consume all server hardware resources and make servers inoperable [14]. Within this category, a well known example is the TCP SYN Flood attack, whereby malicious actors take advantage of the TCP handshake mechanism to create new connections with spoofed SYN packets and never finalize these connections, forcing the target server to hold resources for each incomplete connection [15]. Application Layer attacks on the other hand, are focused directly on the service or application vulnerabilities, rendering the service or application unstable and denying access to users who are the rightful users of the service. Insidious attacks, that often require a small amount of well crafted low rate of write requests that look like that genuine access pattern often manage to bypass a standard detection systems [16]. For illustration, the Slowloris attack, sends partial HTTP requests intermittently in an effort to make connections to servers linger, and take up connections so that the server can create new responses. Since the attack has low bandwidth consumption, it is very hard to catch and with difficulty to detect since DDoS does not bring down the traditional DDoS signatures because there are no typical traffic peaks [17,18]. Comprehensive exploration of these attack vectors is a necessity in the academic discourse to create necessary countermeasures. While application layer attacks can be nuanced and necessitate sophisticated monitoring technology to differentiate between legitimate and suspicious requests, protocol based attacks put severe stress on a service by way of unexpected resource requests. The tactics employed by DDoS attackers also continue to evolve, and this will challenge the network security research & development infrastructure to protect against some significantly sophisticated and dynamic threats. This provides a context to understand the detailed vulnerability and risk analysis of deep learning models for DDoS detection.

2.2. Discussion on challenges of implementing deep learning for DDoS detection

Integrating deep learning (DL) into DDoS detection poses significant challenges well beyond computational power. When implementing deep learning models in dynamic environments or those having high traffic volumes like cloud computing, significant memory and processing resource are required. As a result, general-purpose processors are limited

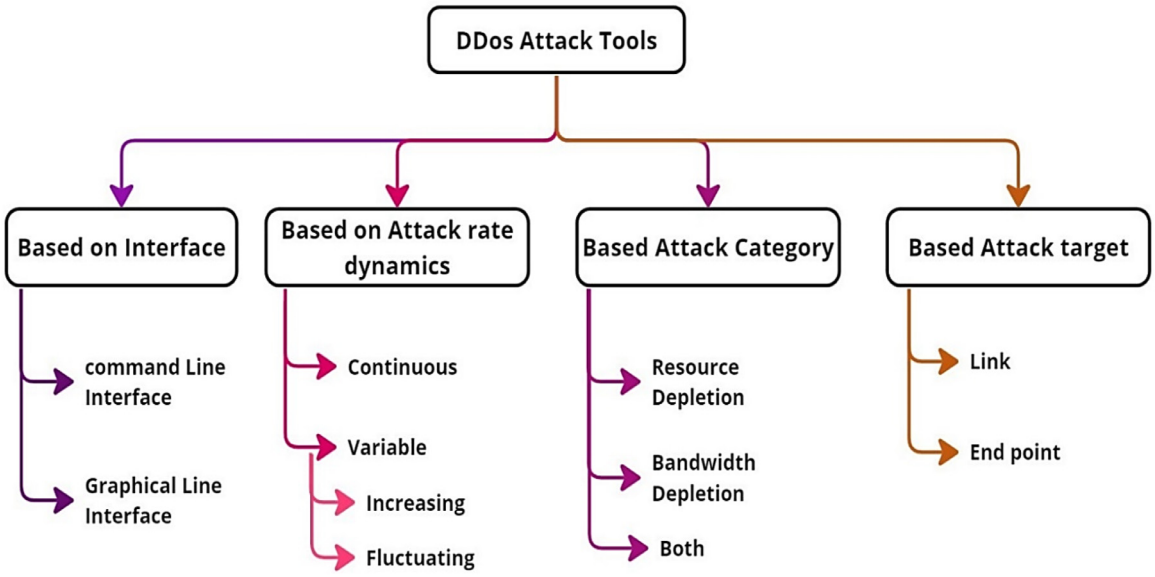

Fig. 1. Taxonomy of DDoS attacks.

in their ability to execute the training process at scale, and due to the large-scale datasets involved in this type of work, GPUs or some other dedicated hardware accelerator is often required in order to make it run efficiently. Further, with real-time detection things are even more complex: the model capable in principle of processing the incoming traffic must simultaneously have low latency, maintain high accuracy, and is agile. To meet these needs, it is essential that the model is updated continuously and retrained to take account of each new wave DDoS tactics. In addition, the deployment and maintenance of these systems requires staff with expertise in both areas increasing operational overhead for any given organizational architecture. Another problem is the high potential for overfit in models learned against static datasets as well as requirement that they integrate seamlessly into existing security systems. All these factors are contributing to ensure that DL-based solutions for countering DDoS attacks are effective in realistic situations.

A multimodal machine learning approach has been proposed for IoT DDoS attack detection [19]. A complete data preparation technique, a dynamic method for picking relevant characteristics to expedite training, and a classifier that can discriminate benign and malicious traffic are included. This system was tested utilizing CICI IDS 2018 datasets and five machine learning classifier

Focusing on application layer DoS attacks, MQTT is being targeted [20]. Researchers created a detection architecture to assess MQTT brokers' resilience and ability to withstand such attacks. A unique method using IoT honeypots to train machine learning algorithms for malware detection uses honeypot interactions' rich datasets [21].

2.3. Comparison of deep learning models

Several deep learning models have been applied to DDoS detection, each with its own strengths and limitations:

- Convolutional Neural Networks (CNNs): Be excellent in recognizing spatial traffic patterns and are particularly powerful when extracting feature from raw traffic flows. However, CNNs may struggle to capture temporal dependencies in sequential data namely, attack patterns slow this over time.
- Long Short-Term Memory (LSTM) Networks: LSTMs are particularly suitable for analyzing traffic time-series data, which makes them well-suited for deserving an evolving attack that unfolds over time. Matching sequential traffic data with it, however, costs more computationally in comparison to CNNs.
- Autoencoders: These models are used for unsupervised anomaly detection, where the model learns to reconstruct normal traffic patterns and flags deviations as potential attacks. Autoencoders are efficient in detecting novel attacks but may require fine-tuning to reduce false positives.
- Recurrent Neural Networks (RNNs): Like LSTMs, RNNs handle sequential data but they are susceptible to the vanishing gradient problem, which limits their power in identifying long term dependencies.

By comparing these models in terms of accuracy, computational efficiency, and suitability for various attack types, researchers can select the optimal approach based on the specific requirements of their cybersecurity infrastructure.

2.4. Explainable AI and deep learning for DDoS attack detection

To improve the transparency and interpretability of AI models, especially in fields like cyber security in which it is so essential how decisions are reached Explainable AI (XAI) is therefore critical. For example, while deep learning models have proven highly effective at detecting Distributed Denial of Service (DDoS) attacks because of their ability to process huge amounts of data at high speed, the fact that they are "black boxes" causes great difficulty for cyber security professionals looking into what their predictions mean.

XAI helps bridge this gap by revealing which features, such as traffic volume or IP patterns, a deep learning model uses to detect DDoS attacks. This interpretability not only builds trust but also aids security teams in refining the models for better accuracy and reliability. Additionally, XAI plays a vital role in the response phase by helping security teams quickly identify and isolate the specific attack vectors, allowing for more focused and efficient mitigation strategies.

Decentralized Federated Learning (DFL) may improve IoT network fault tolerance, minimizing targeted attacks and network management [19]. The approach requires effective model aggregation and communication overhead management. This approach prioritizes node diversity, communication, and model performance.

Semi decentralized algorithms may improve convergence rates and reduce global update bias in federated learning applications [22]. The FL-EOCD approach also provides energy efficient decentralized aggregation in device to device networks [23]. Further research proposes a hybrid strategy integrating device to server and device to device interactions to balance resource variations and device proximity in train-

ing models [24]. Permissioned blockchain technology has been used to solve federated learning synchronization problems, however its scalability and adaptability need further study [25].

Empirical investigations into DDoS detection have utilized various machine learning algorithms to assess their efficacy. One study deployed entropy based measures with KNN classifiers to pinpoint flood attacks, achieving a high degree of accuracy with the CAIDA2007 dataset [26]. Others have enhanced SVM models with genetic algorithms and kernel principal component analysis, reporting near perfect detection rates [27]. Comparative analyses have revealed SVM's superiority in terms of both accuracy and detection speed [28], while feature selection methods have bolstered the efficiency of KNN algorithms [29]. Some research has integrated Naive Bayes classification with an external ML server to analyze incoming traffic, highlighting areas for improvement based on accuracy rates [30]. A tripartite module system has also been proposed, yielding high accuracy rates for classifying DDoS attack types [31].

Through this comprehensive analysis, these studies collectively emphasize the diverse applications and the performance of various machine learning and deep learning techniques in the context of DDoS attack detection. However, they also point to the necessity for continued research to overcome challenges in custom model development, real time detection capabilities, and the impact of algorithmic adjustments on overall system performance. As we advance our review, it is crucial to consider how these methodologies can be refined and integrated into robust defense mechanisms against DDoS attacks within the ever evolving landscape of IoT and cloud computing.

Within the landscape of network security, a novel approach to DDoS attack detection in software defined networks (SDNs) has been articulated [32]. The researchers advanced the traditional

K-nearest neighbors (KNN) algorithm, tailoring it to more precisely assess and identify the signatures of DDoS activities. Their new method was empirically proven accurate, demonstrating its SDN protection potential.

Another group of academics suggests fusing a fuzzy Q-learning system into cloud computing defenses to improve DDoS protection [33]. This combination gives cloud defenses dynamic learning, proposing a new way to protect cloud services from such ubiquitous assaults.

Lucid, a custom deep learning model, advances DDoS assault detection [34]. Performance studies show that Lucid's cybersecurity effectiveness is enhanced by using convolutional and recurrent neural networks to improve detection precision.

Researchers are utilizing machine learning to detect DDoS threats in Industry 4.0′s.

Cyber Physical Production Systems (CPPSs) [35]. CPPSs have shown promise using a unique feature selection approach and advanced algorithms like random forest and high gradient boosting.

Apache Spark has also been used to improve DDoS detection in private cloud systems, particularly OpenStack powered ones [36]. The study shows the framework's ability to detect DDoS threats in cloud infrastructure quickly and accurately.

Another novel study used cloud computing to improve DDoS detection and response [37]. This system uses machine learning and cloud scalability to defend against DDoS attacks, demonstrating the benefits of cloud enabled security. The invention of RT-AMD, a real time cloud monitoring and detection model, advances ML powered cybersecurity solutions [38]. This model shows how machine learning algorithms can detect DDoS flood attacks quickly and accurately. Additionally, BARTD, a bioinspired anomaly based model, may detect App DDoS attacks [39]. Evidence suggests this model's precision and effectiveness in combating subtle application layer threats using bioinspired algorithms and machine learning.

Machine learning based frameworks for identifying DDoS threats in cloud platforms have been further explored, utilizing decision trees and SVMs to fortify cloud security [40]. The architecture is proven to protect cloud computing services against DDoS attacks. Finally, banks' use of IoT based monitoring systems has led to DDoS detection using machine learning models [41]. Results from finance industry IoT networks have shown the usefulness of random forest and KNN models.

Collectively, these studies [32–41] provide a panoramic view of current advancements in DDoS detection techniques. They combine classic algorithms with novel learning models to provide a complete DDoS toolkit for varied network architectures. These findings enable further research into more resilient and adaptive cybersecurity systems as the field evolves.

Research has shown that organizations' growing dependence on cloud infrastructure and the rising threats of data security and privacy necessitate sophisticated detection systems in cloud computing security [42]. An novel method combines filtering and automatic feature selection models to extract attack detection feature sets. The suggested ensemble classifier, which combines machine learning and deep learning models, has performed well in precision, recall, and

F-measure across numerous datasets, suggesting its ability to recognize distinct attack types.

Modern cyberattacks are complicated, requiring security services to protect data privacy, availability, and integrity [43]. This discussion has examined signature based and anomaly based intrusion detection systems for cybercrime. The study cataloged current IDS and examined sophisticated attacker strategies to escape detection.

Researchers have also examined the issues of quality of service (QoS) based filtering in the rapidly growing field of cloud service selection [44]. Users struggle to evaluate cloud services using performance measures due to personal preferences. Weighted summing methods may misinterpret QoS attribute relationships, resulting in misleading results.

The Fuzzy Analytic Hierarchy Process prioritizes QoS standards in the complex cloud service environment [45]. This technique, together with TOPSIS, evaluates cloud services comprehensively, helping customers make decisions.

Cyberattacks on smart grids have spurred a research on IDS effectiveness [46]. This study used feature selection and hyperparameter optimization to improve detection and compared typical machine learning models based on performance criteria. The Categorical Boosting classifier outperformed other models, creating a standard for intrusion detection.

A study on the COVID-19 pandemic highlighted cloud computing's role in remote work and communication [47]. With cloud computing at the forefront of IT innovation, the study underscored the growing necessity for secure, scalable, and efficient cloud solutions.

Moreover, the challenge of processing vast amounts of security related data, crucial for network intrusion detection, was addressed by leveraging Apache Spark's processing capabilities [48]. A hybrid intrusion detection method combining deep neural networks with machine learning techniques was proposed to enhance the detection accuracy.

Finally, targeting the pressing issue of DDoS attacks in cloud environments, a study introduced a novel classification method supported by an efficient feature selection process and an advanced deep learning based classifier model [49]. Utilizing the KDD'99 dataset, the study validated the model's effectiveness, reporting significant improvements in detection metrics over traditional RBM models.

These diverse studies [42–49] reflect the multifaceted nature of cloud security challenges and underscore the innovative solutions being developed to address them. As cloud computing becomes increasingly integral to organizational operations, the enhancement of security measures to protect against sophisticated cyber threats remains a pivotal concern. This review analyzes these contributions, highlighting the progress and identifying areas for further exploration to bolster cloud computing security in an ever evolving digital landscape. Table 1 summarizes the analysis of previous investigations.

The extensive review of related works in the literature on DDoS attack detection and cloud computing security provides a broad spectrum of insights and trends that are critical to understanding the advancements in this field as shown in Table 1. Research presented in reference [19] delves into machine learning based DDoS detection within

Table 1
Analysis of related work.

Reference	Methodology	Key findings	Resolved issues
[19]	ML-based approach for DDoS detection in IoT networks. Includes data preprocessing, dynamic feature selection, and classification. Evaluated on CICI IDS 2018 datasets with five ML classifiers.	Effective DDoS detection in IoT networks with high accuracy using the proposed methodology.	Improved detection accuracy for IoT DDoS threats, addressed dataset imbalance.
[20]	Detection architecture for application layer DoS attacks, focusing on MQTT protocol. Evaluates operational impact and detection capability.	Successful identification of application layer DoS attacks with insights into operational impact.	Enhanced detection of application-layer DoS attacks on specific IoT protocols.
[21]	Honeypot-based method using ML algorithms to detect malware in IoT. Utilizes IoT honeypot data for dynamic and efficient model training.	Efficient detection of malware in IoT environments using honeypot-based data and ML algorithms.	Enabled real-time malware detection in IoT environments using honeypots.
[22]	Semi-decentralized federated learning algorithm with central parameter server for sporadic connectivity.	Improved convergence speed and reduced variance in semi-decentralized federated learning.	Addressed convergence speed and global update bias in federated learning.
[23]	Federated Learning Empowered Overlapped Clustering for Decentralized Aggregation (FL-EOCD) approach using device-to-device communication. Focus on energy-efficient framework.	Energy-efficient federated learning with device-to-device communication and overlapping clusters for decentralized aggregation.	Improved energy efficiency in federated learning with device-to-device interactions.
[24]	Semi-decentralized learning approach with local training and device-to-device interactions among clusters of devices.	Local training and device-to-device interactions for improved federated learning. Challenges in scalability and overhead.	Addressed overhead in federated learning but with scalability challenges remaining.
[25]	Asynchronous federated learning aggregation protocol using a permissioned blockchain framework.	Mitigation of synchronization issues in federated learning using blockchain. Challenges in real-world edge computing scenarios.	Solved synchronization issues in federated learning, with scalability requiring further study.
[26]	Entropy and logarithmic measures to detect TCP SYN/ICMP flood attacks in SDNs using K-nearest neighbors (KNN).	High accuracy in detecting flood attacks in SDNs with KNN algorithm.	Enhanced detection accuracy for TCP SYN/ICMP flood attacks in SDNs.
[27]	Enhanced SVM model integrating genetic algorithms (GA) and KPCA for DDoS attack detection.	Highly accurate DDoS attack detection with optimized SVM parameters using GA.	Significantly improved detection accuracy using SVM with GA and KPCA.
[28]	Comparative analysis of seven classifiers, with SVM outperforming others in accuracy and detection speed.	SVM as the top-performing classifier with high accuracy in DDoS attack detection.	Established SVM as the most accurate model for DDoS detection in comparative analyses.
[29]	Feature selection methods and KNN with wrapper-based feature selection approach for DDoS attack detection.	KNN with feature selection achieving high accuracy in detecting DDoS attacks.	Enhanced KNN's detection performance using feature selection.
[30]	Scenario involving four interconnected ISPs and Naive Bayes (NB) classification. ML server for analyzing features from incoming packets.	NB-based classification with moderate accuracy for detecting anomalies in network traffic.	Highlighted areas for accuracy improvement in Naive Bayes classification for DDoS detection.
[31]	Tripartite module system (TCFI, FE, TC) for DDoS attack classification.	Achieved high accuracy rates for DDoS attack and binary classification.	Provided highly accurate DDoS attack classification exceeding 95%.

(*continued on next page*)

Table 1 (*continued*)

Reference	Methodology	Key findings	Resolved issues
[32]	Enhanced K-nearest neighbors (KNN) algorithm for accurate DDoS attack detection in software-defined networks (SDNs).	Improved accuracy in detecting DDoS attacks using an enhanced KNN algorithm in SDNs.	Boosted DDoS detection accuracy in SDNs with enhanced KNN.
[33]	Integration of fuzzy Q-learning algorithm for DDoS attack defense in cloud computing environments.	Reinforcement learning-based defense against DDoS attacks in cloud computing.	Provided dynamic learning-based protection for cloud services.
[34]	Lucid deep learning model for DDoS attack detection using convolutional and recurrent neural networks.	Efficient DDoS attack detection with Lucid deep learning model.	Improved detection accuracy with convolutional and recurrent neural networks.
[35]	ML-based feature selection and random forest for DDoS attack detection in Cyber Physical Production Systems (CPPSs).	Effective DDoS attack detection in CPPS environments using ML techniques.	Enhanced detection efficiency in CPPSs using ML feature selection.
[36]	DDoS attack detection in private clouds, specifically on OpenStack, using Apache Spark and ML algorithms.	Apache Spark-based detection of DDoS attacks with ML algorithms in private cloud environments.	Enabled faster and more accurate DDoS detection in OpenStack-powered private clouds.
[37]	Cloud-based detection and mitigation of DDoS attacks using cloud resources and ML.	Efficient detection and mitigation of DDoS attacks using cloud-based resources and ML.	Improved scalability and detection performance in cloud-based DDoS mitigation.
[38]	RT-AMD model for real-time DDoS flood attack monitoring and detection in cloud computing. Utilizes ML algorithms.	Real-time detection and response to DDoS flood attacks in cloud computing using the RT-AMD model.	Advanced real-time DDoS detection and response capabilities in cloud environments.
[39]	BARTD bio-inspired anomaly-based approach for detecting application layer DDoS attacks.	Effective detection of application layer DDoS attacks using the BARTD bio-inspired approach.	Improved precision in detecting subtle application-layer DDoS threats.
[40]	ML-based framework using decision trees and SVM for DDoS attack detection in cloud computing.	Improved cloud computing security with DDoS attack detection using the ML-based framework.	Enhanced cloud security through decision tree and SVM-based detection.
[41]	Detection of DDoS attacks in IoT-based monitoring systems in the banking industry using ML models.	ML-based models for accurate detection of DDoS attacks in IoT networks in the banking sector.	Increased detection accuracy for IoT-based DDoS threats in financial systems.
[42]	Ensemble classifier with feature selection for cloud security using CSA.	Highly accurate cloud security using an ensemble classifier with feature selection.	Improved cloud security using an ensemble classification approach.
[43]	Review of intrusion detection strategies, focusing on signature-based and anomaly-based IDS.	Comprehensive overview of intrusion detection strategies with insights into challenges.	Provided insights into the challenges of modern intrusion detection systems.
[44]	Method for selecting cloud services considering user preferences and QoS constraints.	User-centric cloud service selection method accounting for QoS preferences.	Addressed challenges in selecting cloud services based on QoS constraints.
[45]	Rating cloud services based on QoS standards using Fuzzy Analytic Hierarchy Process (Fuzzy AHP).	Methodology for rating cloud services considering QoS standards and user preferences.	Improved decision-making process for selecting cloud services using Fuzzy AHP.
[46]	Comparison of machine learning models for network intrusion detection in smart grids using the KDD'99 dataset.	Comparison of ML models for network intrusion detection in smart grids with a focus on accuracy and false alarms.	Enhanced network intrusion detection with optimized ML model comparison.
[47]	Evaluation of cloud computing security, emphasizing the importance of secure remote access and data processing capabilities.	Importance of cloud computing in modern life and evaluation of cloud computing security.	Highlighted the critical role of cloud security for remote access and data processing.
[48]	Apache Spark-based hybrid approach combining deep neural networks and machine learning for network intrusion detection.	Efficient data processing and network intrusion detection using Apache Spark and hybrid ML/DL models.	Improved intrusion detection accuracy and data processing with hybrid methods.
[49]	Classification method for DDoS attack detection using feature subset selection with Random Harmonic Search and RBM model in cloud environments.	High detection accuracy for DDoS attacks in cloud environments using feature selection and RBM model.	Enhanced detection accuracy for cloud-based DDoS detection with feature selection.

IoT networks, adopting a comprehensive approach that includes data preprocessing, dynamic feature selection, and classification to enhance detection capabilities. Another study in [20] tackles application layer DoS attacks, focusing on the MQTT protocol and examining the operational impacts and detection capabilities of various architectures.

A honeypot based methodology for malware detection in IoT environments is proposed in [21], utilizing rich honeypot data to train models dynamically and efficiently. References [22,23], and [24] explore the use of Federated Learning (FL) for DDoS detection, discussing semi decentralized FL algorithms, energy efficient frameworks, and device to device communication enhancements.

The work in [25] introduces an asynchronous federated learning aggregation protocol that employs a permissioned blockchain framework to address synchronization challenges, particularly in edge computing scenarios. Several studies ([26,27,28,29,30,31]) investigate various machine learning and deep learning approaches, including SVM, K-nearest neighbors (KNN), and Naive Bayes, for DDoS detection, focusing on feature selection methods to achieve high detection accuracy.

Particularly, [27] integrates genetic algorithms and kernel Principal Component Analysis with SVM models to achieve near perfect detection accuracy. The importance of utilizing real world datasets like the KDD'99 and CICI IDS 2018 for model evaluation is highlighted in references [26,31], and [36].

Cloud based DDoS detection strategies are explored in [37,38], and [39], leveraging cloud resources and machine learning to scale and mitigate attacks effectively. The BARTD model in [39] exemplifies anomaly based detection approaches, while bio inspired algorithms are also discussed for precise threat identification.

Studies [42,43], and [44] address various aspects of cloud computing security, with [42] introducing an ensemble classifier that enhances robustness through feature selection. In the context of IoT, [46] evaluates machine learning models for intrusion detection in smart grids, emphasizing the security of IoT based systems.

The relevance of cloud computing in contemporary settings, particularly highlighted during the COVID-19 pandemic, is underscored in [47], focusing on security, data privacy, and processing efficiency. Apache Spark based methods for handling large volumes of security related data and enhancing network intrusion detection through hybrid ML,DL models are discussed in [48].

Finally, [49] presents a novel classification method for DDoS attack detection in cloud environments, emphasizing the role of feature selection and RBM models to achieve high accuracy. This collection of studies presents a rich landscape of research addressing critical issues in DDoS attack detection and cloud computing security.

While deep learning offers a powerful approach to DDoS detection, alternative mitigation strategies are worth considering. Traditional signature-based methods, which rely on predefined patterns to identify known attacks, remain effective against specific threats but struggle with unknown or evolving attack vectors. Anomaly-based detection systems, which monitor network traffic for deviations from normal patterns, offer better adaptability to new attacks but are prone to higher false-positive rates. Rate-limiting, traffic filtering, and the use of scrubbing centers are practical approaches that reduce the impact of volumetric attacks by managing traffic flow. A hybrid approach combining deep learning with these methods can enhance the robustness of DDoS defense systems [50]. For example, deep learning could be used for anomaly detection, while signature-based methods filter known threats, creating a multi-layered defense strategy that adapts to the dynamic nature of modern DDoS attacks.

In conclusion, the field of DDoS attack detection and cloud computing security is vibrant and evolving. Researchers are leveraging a range of techniques, from machine learning and deep learning to bio inspired algorithms and federated learning, to address the growing challenges posed by cyber threats. The choice of methodology often depends on the specific application, network environment, and the need for real time detection. Real world datasets play a crucial role in evaluating the effectiveness of detection models. As cloud computing continues to shape modern IT infrastructure, ensuring robust security measures remains a paramount concern, and ongoing research in this area is essential to stay ahead of evolving cyber threats.

3. Dataset used in DDoS

Defects in testing and validation datasets must be acknowledged to rigorously evaluate IoT DDoS attack detection technologies. The findings of CIC IDS2017 [51], CICDDoS2019 [52], UNSW-NB15 [53], and NSL KDD are limited by the lack of authentic IoT cases. Despite their widespread use in research, Bot-IoT and IoTID20 have a large imbalance between harmful and benign traffic representations. Over 99% of the Bot-IoT dataset is hostile attack data, which does not reflect network traffic realities. This mismatch can cause models to detect attacks well but not typical behavior, resulting in high false, positive rates. Some statistics omit DDoS attack types, which is unfortunate given their ubiquity and research focus. While Bot-IoT [54] and IoTID20 [55] show a small DDoS attack scope, demonstrating the need. for datasets that encapsulate a broader spectrum of DDoS methodologies to enhance the detection and generalization capabilities of the models.

In terms of methodological advancements, the application of machine learning algorithms such as XGBoost and AdaBoost in the realm of DDoS detection within IoT networks remains limited [56]. XGBoost, recognized for its performance and computational efficiency, could significantly contribute to the processing and analysis of the vast quantities of data inherent to IoT. This suggests a potential avenue for future research to leverage these algorithms, which could lead to the development of more sophisticated and effective detection models.

An analysis of the current state of datasets and methodologies reveals a critical need for more realistic and balanced datasets that reflect the heterogeneity of network traffic and for the exploration of underutilized, yet powerful, machine learning techniques. Addressing these gaps could yield significant improvements in the reliability of DDoS attack detection systems, fortifying the security framework within the rapidly expanding domain of IoT [57–59].

The problem is that the datasets are of poor quality and unbalanced on ATT-IOT for developing effective DDoS detection models, particularly when it comes to IoT networks. Under these circumstances, any unrepresented attack types will simply go undetected with these biased models. Therefore, robust machine learning techniques such as decision trees, ensemble methods and support vector machines can both improve classification accuracy and alleviate imbalance. For instance, five machine learning algorithms were used to make optimistic predictions on the BOT-IOT data in a recent study [64]. However, in this work, deep learning models are "black boxes" meaning they are difficult to understand and trust. As such, this necessitates the development of explainable AI (XAI) for better comprehension and faith in the machine in question. Also, the complexity of real-time detection in an IoT environment demands high-efficiency AI systems capable of processing immense, diversified data. Ultimately, embedding deep learning in a large-scale cross-sectional-longitudinal platform is the best means for preserving both scalability and flexibility whilst keeping up with tasks related to new threats.

Fig. 2, labeled "Dataset Taxonomy," shows a classification of various cybersecurity datasets around a central node titled "Dataset." From this central point, branches extend to different sub-categories of datasets. These branches include datasets like KDD Cup99, IoTID20, BOT-IoT, Ton_IoT, and CCD-INID-V1, which are typically used in network intrusion detection and IoT security research. Another branch leads to NSL-KDD and UNSW NB15, noted for their application in network intrusion detection system (NIDS) studies. Additional branches identify datasets such as N-BaIoT2018, associated with IoT security, and CIRA-CIC-DoHBrw-2020 and CIC-DDoS-2019, focused on DNS security and DDoS attack research. Lastly, the diagram includes CSE-CIC-IDS2018, another significant dataset for intrusion detection systems. This taxon-

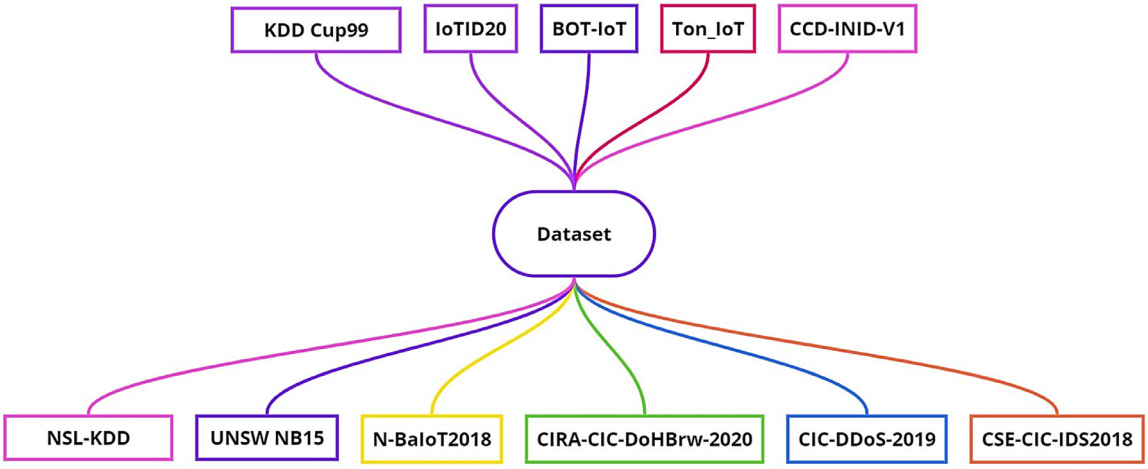

Fig. 2. Dataset taxonomy.

Table 2
Compendium of IoT-Related DDoS detection datasets.

Dataset Title	Issued Year	Key Hardware Elements	Software Employed	IoT Traffic	Primary Challenges and Gaps
CCD-INID-V1	2021	Smart sensors, Raspberry Pi, Rainbow HAT	Network monitoring with Wireshark	Yes	Only DoS focus; lacks varied internet use cases
TON_IoT	2020	Various smart devices	Network tools like Nmap	Yes	Data is unbalanced; lacks proper validation
CIC-IDS2017	2017	Network infrastructure devices	Variety of intrusion detection tools	No	High volume and class imbalance; non-IoT centric
BOT-IoT	2019	Virtual machines, firewalls	DDoS simulation tools	Yes	Coverage of DDoS types is limited; class imbalance
IoTID20	2020	Diverse smart home devices	N/A	Yes	Focuses only on Mirai; class imbalance issues
CSE-CIC-IDS2018	2018	AWS platform, computer stations	Flow and attack analysis tools	No	Seven different attack scenarios; not IoT specific

omy effectively organizes and distinguishes datasets based on their specific research applications in cybersecurity.

Table 2 presents a summary of various IoT-related DDoS detection datasets, including their titles, issue years, key hardware and software components, whether they include IoT traffic, and the primary challenges associated with each dataset. The datasets listed are CCD-INID-V1 (2021), TON_IoT (2020), CIC-IDS2017 (2017), BOT-IoT (2019), IoTID20 (2020), and CSE-CIC-IDS2018 (2018). They range from utilizing smart sensors and Raspberry Pi to AWS platforms and include both specific IoT devices and more general network infrastructure. Software tools used in these datasets vary from network monitoring tools like Wireshark to intrusion detection tools and DDoS simulation tools. The challenges highlighted across these datasets include class imbalance, focus on specific DDoS types like Mirai, lack of varied internet use cases, and non-IoT centric data issues. Some datasets also suffer from data imbalance and lack proper validation mechanisms.

In order to improve the databases required for DDoS detection, it will be necessary to use several strategies. One of the main problems in present databases is an imbalance in types of data, where attack records overwhelm normal traffic and thus the model is biased. Such models are good at detecting attacks, but when confronted with ordinary events they fail dismally. To address this, future datasets should reflect the real world likely attack-to-benign traffic ratios more accurately. Data augmentation techniques, such as generating synthetic non-attack data, can help to balance the datasets. Furthermore, current databases contain a deficiency in the variety of attack types involving IoT devices, with their unique vulnerabilities and communication protocols. Constructing datasets rich in attack vectors that cover a broader range, applications and protocols as well as volumes and levels, and introducing non-sugar coded, IoT-specific traffic will raise the commonality of the models. Lastly, taking data from actual networks–instead of artificially controlled surroundings–yields richer measurements for both model training and evaluation.

Table 3 categorizes different sectors by the average size of DDoS attacks they face (measured in Mbps), the number of attacks, and provides a brief description of each sector's experience. For instance, the consulting sector experiences moderate attack sizes (10,000 Mbps) and a relatively low number of attacks (25), while the health care sector encounters the highest average attack size (70,000 Mbps) with a moderate number of attacks (60). The ISP/Hosting sector faces both high attack sizes (25,000 Mbps) and the highest number of attacks (400), indicating significant vulnerability. On the other end, the utilities sector sees very small attack sizes (2000 Mbps) with the lowest number of attacks (10). Each sector's description reflects its specific challenges related to DDoS threats, ranging from small to very large attack sizes and varying frequencies of attacks.

Fig. 3 illustrates the considerable variability both in size of attacks and number of attacks across a range of different sectors. The healthcare sector experiences the highest average attack size. At 70,000 Mbps, this indicates a heightened risk of large-scale attacks targeting critical infrastructure. By contrast, ISP/Hosting endures the most attacks in totality. It has 400 attacks, reflecting the inherent vulnerability of this sector as it manages much network traffic. With the smallest average attack size and the fewest number of attacks, the utilities sector presents a relatively low threat level. And sectors such as telecommunications, transportation fruit high numbers of attacks–emphasizing how crucial

Table 3
Datasets sectors and description.

Sector	Average attack size (Mbps)	Number of attacks	Description
Consulting	10,000	25	The consulting sector experiences moderate attack sizes with a relatively low number of attacks.
Education	15,000	40	The education sector has a higher average attack size with a moderate number of attacks.
Finance	8000	30	The finance sector sees smaller attack sizes but a considerable number of attacks.
Gaming	5000	20	The gaming sector experiences relatively low attack sizes and a lower number of attacks.
Government	3000	20	Government sector faces small attack sizes with a lower number of attacks.
Health Care	70,000	60	The health care sector has the highest average attack size with a moderate number of attacks.
ISP/Hosting	25,000	400	ISP/Hosting sector faces high attack sizes and the highest number of attacks.
Media & Entertainment	60,000	100	Media & Entertainment sector has large attack sizes and a significant number of attacks.
Retail	3000	25	The retail sector experiences small attack sizes with a relatively low number of attacks.
Technology	15,000	50	The technology sector sees higher attack sizes and a moderate number of attacks.
Telecommunications	20,000	350	Telecommunications sector faces large attack sizes and a high number of attacks.
Transportation	10,000	300	The transportation sector has moderate attack sizes with a high number of attacks.
Utilities	2000	10	The utilities sector experiences very small attack sizes and the lowest number of attacks.
Manufacturing & Construction	5000	20	Manufacturing & Construction sector faces relatively low attack sizes and a lower number of attacks.

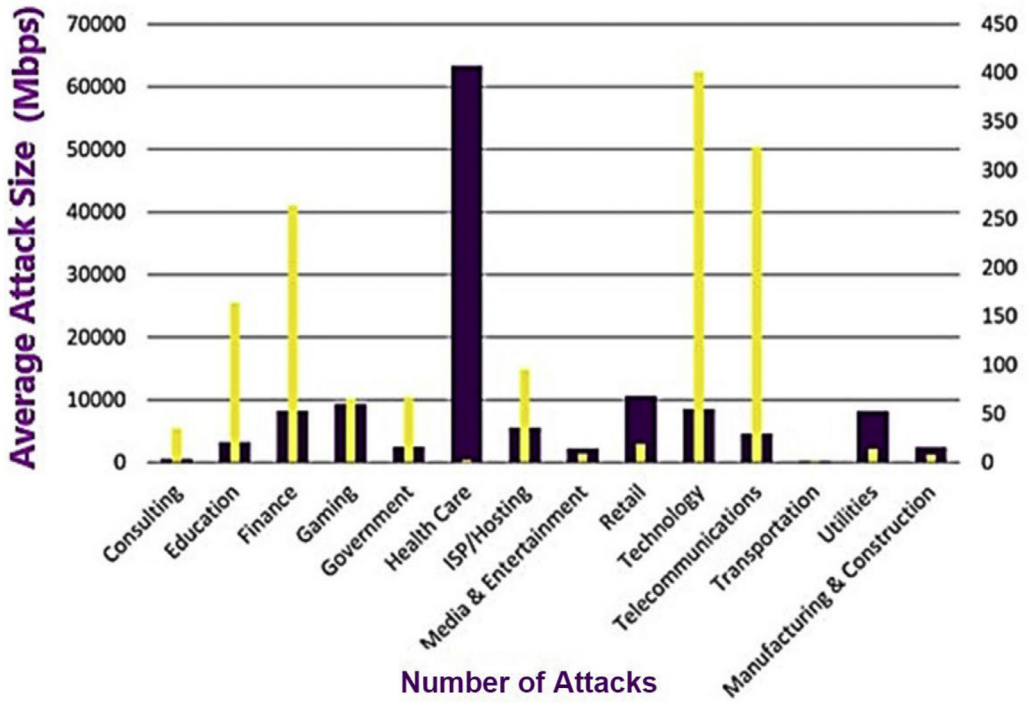

Fig. 3. A comparison of average DDoS attack size and frequency across various sectors, highlighting sector-specific vulnerabilities and the need for tailored DDoS mitigation strategies.

their infrastructures are. This variability suggests that defense strategies must be tailored, with robust bandwidth management needed for high-volume attacks while sectors under frequent but smaller attacks could benefit from more detailed traffic-level detection techniques. The visualization shows both the changing nature of DDoS threats and the need for mitigation geared to particular sectors in its fading colours and shapes.

There is a clear distinction between the datasets used to detect DDoS attacks with some including IoT-specific traffic and others not. The majority of the five datasets lack any sign of IoT traffic; this means they are more general by nature and so more directly applicable to other network environments. By contrast, only one dataset focuses explicitly on IoT traffic, which demonstrates that what public datasets are available for IoT environments is still quite scarce indeed. This disparity then marks a well behind in terms of data available for studying DDoS attacks unique to IoT environments where special problems arise in dataset development and analysis.

The illustration in Fig. 4 demonstrates what DDoS attack types the SOC team observed from Q1 2020 to Q1 2021. The of volumetric DDoS attack most frequent Volumetric DDoS attacks stack up when it comes off the peak, with over 1000 incidents in the first quarter of 2020 alone. Conversely, protocol DDoS attacks and application DDoS attacks both accounted for considerably fewer incidents. The study observed a higher but toppling low point for attack upon protocol during this time period span that has a relatively stable and steady flow. The diagram shows that within one DDoS event, several tactics may be used to make up over the overall total more than 100 %. It is important to make this point clear in order not to confuse the data or ensure the multifaceted character of DDoS attack methods, which often strike at various layers of network and application infrastructure. Furthermore, the figure does not expound on how these attacks will affect network performance or application availability, making an important part of study unaddressed.

This Fig. 5 shows the distribution of application layer DDoS attacks for several months. This segment recorded the highest number of attacks

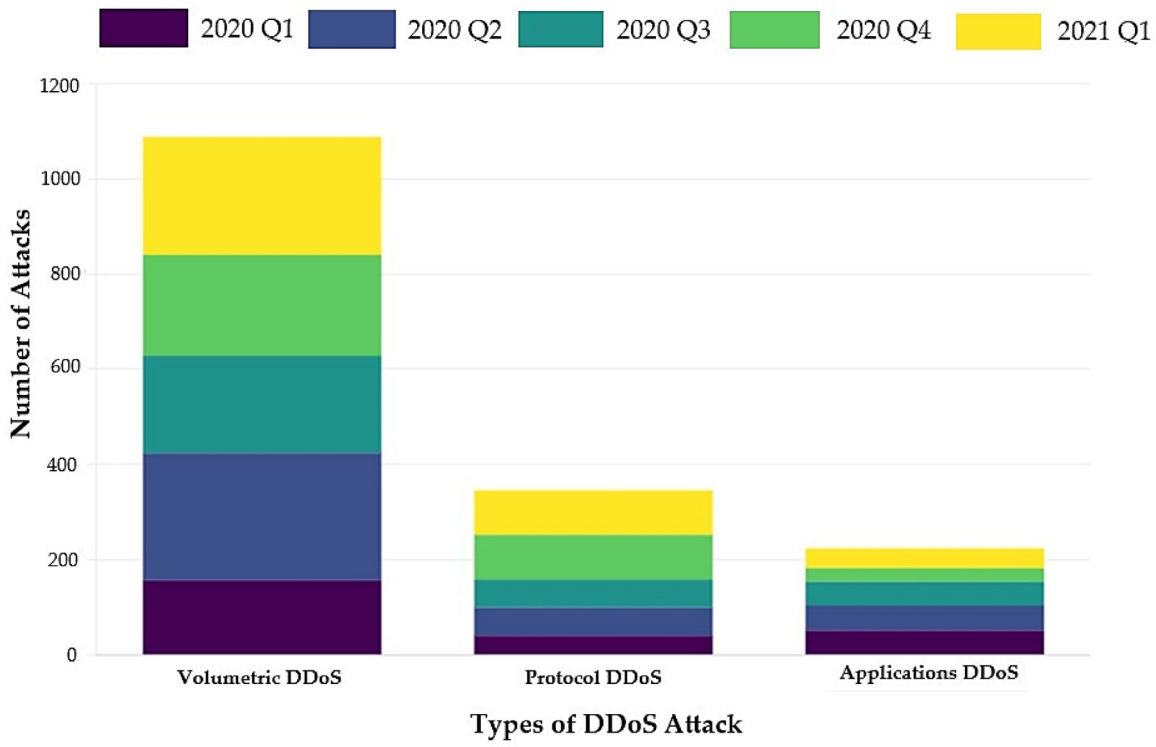

Fig. 4. Frequency of DDoS attack types, January 2020 through March 2021.

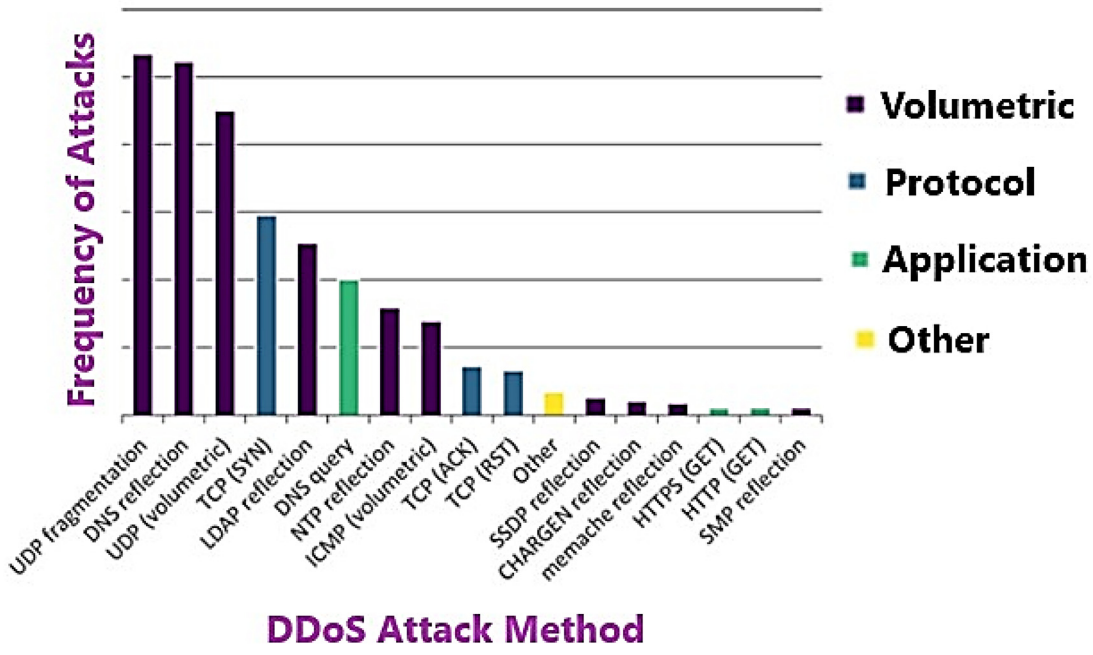

Fig. 5. Frequency of different DDoS attack tactics, January 2020 through March 2021.

in the last year in Q1 2022, with a 164% year on year surge in attacks and a 135% quarter on quarter increase, respectively. In fact, the volume of HTTP DDoS attacks for March surpassed the volume of incidents recorded for the entirety of Q4 2021, Q3 2021, and Q1 2021 combined.

Table 4 outlines recent scholarly work on using deep learning methods for DDoS detection. The articles range from systematic reviews of the field to specific implementations for edge devices and application layers. The first entry by Mittal et al., published in Soft Computing 2023, provides a comprehensive review of deep learning in DDoS detection, discussing everything from methodologies to research gaps. Ramanathan and colleagues focus on using Convolutional Neural Networks for detecting attacks on edge systems, as outlined in their arXiv preprint. Asad et al., in the Journal of Big Data, apply Deep Neural Networks to specifically tackle application layer DDoS attacks in wireless networks. Lastly, Hu, Yu, and Shen utilize Long Short Term Memory Networks to analyze flow-level features for DDoS detection, demonstrating high accuracy in their work published in IEEE Transactions on Network and Service Management. Each study contributes to understanding and improving DDoS

Table 4
Related work summarization.

Title	Authors	Publication	Focus	Method	Key Features
Systematic Review on Deep Learning Approaches for DDoS Detection [60]	Meenakshi Mittal, Krishan Kumar, and Sunny Behal	Soft Computing, 2023	Systematic review of deep learning literature related to DDoS detection	N/A	Reviews different types of DDoS attack detection using deep learning, strengths and weaknesses of existing methods, benchmark datasets, preprocessing strategies, hyperparameter values, experimental setups, performance metrics, research gaps, and future directions.
Supervised Deep Learning Solution for DDoS Detection on Edge Systems [61]	Vedanth Ramanathan, Krish Mahadevan, and Sejal Dua	arXiv preprint	Detecting DDoS attacks on edge devices	Convolutional Neural Networks (CNN)	Leverages CNNs for accurate detection and addresses sophisticated cybersecurity attacks.
Deep Learning Techniques for Application Layer DDoS Detection [62]	Asad et al.	Journal of Big Data	Detecting application layer DDoS attacks	Deep Neural Network (DNN)	Uses feed forward back propagation for reliable detection of DoS attacks in wireless sensor networks (WSNs).
Deep Learning Based DDoS Detection Using Flow Level Features [63]	Shun-Yun Hu, Chia-Mu Yu, and Chien-Chung Shen	IEEE Transactions on Network and Service Management	DDoS detection using flow level features	Long Short Term Memory (LSTM) Networks	Utilizes LSTM networks to capture temporal dependencies in network traffic, extracts flow level features such as packet count, byte count, and interarrival time, achieves high accuracy.

detection through advanced deep learning techniques, highlighting the effectiveness of these methods in different network scenarios.

4. Conclusion and future challenges

This review detailed DDoS attacks. Deep learning DDoS detection and mitigation solutions demonstrate cybersecurity's dynamic nature. Despite breakthroughs in conventional and machine learning detection, DDoS attacks are becoming increasingly complicated and elusive [64,65].

In creating and testing DDoS detection models, CIC-IDS2017 and Bot-IoT datasets are crucial. Class imbalance and a lack of representation for IoT specific communications, which attackers are increasingly targeting, are drawbacks. More balanced and realistic datasets are needed to design effective protection mechanisms.

Deep learning may improve DDoS attack detection and response in the future. However, issues remain, such as ensuring openness and trust in automated defensive systems through explainable AI. Integrating deep learning systems into cybersecurity networks requires compute and model maintenance.

AI and ML in cybersecurity will alter DDoS protection. These technologies can greatly improve detection and mitigation measures, but academics, practitioners, and policymakers must work together to overcome the hurdles and capitalise on the prospects.

The rapidly evolving landscape of Distributed Denial of Service (DDoS) attacks is marked by increased complexity and frequency, with a trend towards multi vector attacks and the utilization of IoT devices in botnets. This section delves into the sophisticated, AI driven tactics reshaping the threat landscape.

Deep learning has significantly advanced DDoS attack detection, offering superior accuracy, speed, and adaptability compared to traditional methods. Integrating deep learning into existing network security infrastructures poses a challenge, particularly due to computational complexity, substantial resource requirements, and the need for comprehensive, representative training datasets. Continuous model updates are crucial to counter new DDoS attack variants effectively.

In the field of cybersecurity, the use of artificial intelligence also poses ethical challenges, one of them being that training data are often biased. The consequence is that, where datasets are not balanced, benign traffic will wrongly be identified as malign. This problem becomes especially acute in mixed settings, like IoT networks. In addition, AI systems are vulnerable to adversarial attacks, in which a substitute data pattern deceived the model. This will require Explainable AI (XAI) if we are to inject greater transparency and trust into our systems. Creating ethical AI systems will mean working creatively to reduce the biases inherent in datasets, constantly monitoring their performance, and making models fairer and more explainable.

Explainable AI (XAI) helps DDoS protection deep learning models become more transparent and reliable. For ethical and regulatory compliance, XAI must be implemented to make decision making clear.

Future research focuses on enhancing deep learning models for DDoS detection. Effectively combating DDoS threats requires advanced technologies like federated learning or transfer learning and cross sector collaboration. DDoS defense requires constant modification and learning.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

CRediT authorship contribution statement

Doaa Mohsin Abd Ali Afraji: Writing – original draft, Investigation, Formal analysis, Data curation. **Jaime Lloret:** Writing – review & editing, Supervision, Methodology, Investigation. **Lourdes Peñalver:** Writing – review & editing, Supervision, Investigation.

References

[1] M. Alduailij, Q.W. Khan, M. Tahir, M. Sardaraz, F. Malik, Machine learning based ddos attack detection using mutual information and random forest feature importance method, Symmetry (Basel) 14 (6) (2022) 1095.
[2] S. Velliangiri, P. Karthikeyan, V. Vinoth Kumar, Detection of distributed denial of service attack in cloud computing using the optimization-based deep networks, J. Experiment. Theoretic. Artific. Intell. 33 (3) (2021) 405–424.
[3] G.S. Kushwah, V. Ranga, Optimized extreme learning machine for detecting ddos attacks in cloud computing, Comput. Secur. 105 (2021) 102260.
[4] E. Arul, A. Punidha, Supervised deep learning vector quantization to detect memcached ddos malware attack on cloud, SN Comput. Sci. 2 (2) (2021) 85–112.
[5] J.K. Seth, S. Chandra, An effective dos attack detection model in cloud using artificial bee colony optimization, 3D Res. 9 (3) (2018) 44.
[6] Q. Yan, F.R. Yu, Distributed denial of service attacks in software-defined networking with cloud computing, IEEE Communicat.. Magazine 53 (4) (2015) 52–59.
[7] A.E. Cil, K. Yildiz, A. Buldu, Detection of ddos attacks with feed forward based deep neural network model, Expert Syst. Appl. 169 (2021) 114520.
[8] A.A. Alqarni, Majority vote-based ensemble approach for distributed denial of service attack detection in cloud computing, J. Cyber Secur. Mobil. 12 (2022) 265–278.

[9] R. Doriguzzi-Corin, S. Millar, S. Scott-Hayward, J.Martinez del Rincon, D. Siracusa, Lucid: a practical, lightweight deep learning solution for ddos attack detection, IEEE Transact. Network Serv. Manage. 17 (2) (2020) 876–889.

[10] F. Jiang, Y. Fu, B.B. Gupta, Deep learning based multi-channel intelligent attack detection for data security, IEEE Transact. Sustain. Comput. 5 (2) (2020) 204–212.

[11] A. Al-Abassi, H. Karimipour, A. Dehghantanha, R.M. Parizi, An ensemble deep learning- based cyber-attack detection in industrial control system, IEEE Access 8 (2020) 83965–83973.

[12] Z. Tian, C. Luo, J. Qiu, X. Du, M. Guizani, A distributed deep learning system for web at- tack detection on edge devices, IEEE Transact. Indust. Informat. 16 (3) (2020) 1963–1971.

[13] E. Džaferović, A. Sokol, A.Abd Almisreb, S.M. Norzeli, Dos and DDoS vulnerability of IoT: a review, Sustain. Eng. Innov. 1 (2019) 43–48.

[14] D. Neelam, M. Prasenjit, S. Shashank, K. Rahamatullah, Research trends in security and ddos in sdn, Secur. Commun. Netw. 9 (2016) 6386–6411.

[15] T. Ehrenkranz, J. Li, On the state of ip spoofing defense, ACM Trans. Internet Technol. 9 (2009) 1–29.

[16] R. Vishwakarma, A.K. Jain, A survey of ddos attacking techniques and defense mechanisms in the IoT network, Telecommun. Syst. 73 (2019) 3–25.

[17] S. McGregory, Preparing for the next ddos attack, Netw. Secur. (2013) 5–6.

[18] Y.G. Dantas, V. Nigam, I.E. Fonseca, A selective defense for application layer DDoS at- tacks, in: Proceedings of the 2014 IEEE Joint Intelligence and Security Informatics Conference, 2014, pp. 24–26, doi:10.1007/s00500-021-06608-1.

[19] S. Ullah, Z. Mahmood, N. Ali, T. Ahmad, A. Buriro, Machine learning-based dynamic at- tribute selection technique for DDoS attack classification in IoT networks, Computers 12 (6) (2023) 115.

[20] N.F. Syed, Z. Baig, A. Ibrahim, C. Valli, Denial of service attack detection through machine learning for the IoT, J. Inf. Telecommun. 4 (4) (Oct 2020) 482–503.

[21] R. Vishwakarma, A.K. Jain, A honeypot with machine learning based detection framework for defending IoT based botnet DDoS attacks, in: Proc. 3rd Int. Conf. Trends Electron. Informat. (ICOEI), 2019, pp. 1019–1024. https://ieeexplore.ieee.org/document/10192467.

[22] A. Mihoub, O.B. Fredj, O. Cheikhrouhou, A. Derhab, M. Krichen, Denial of service attack detection and mitigation for internet of things using looking-back-enabled machine learning techniques, Comput. Electr. Eng. 98 (2022) 107716.

[23] J. Kumar, Mitigate volumetric DDoS attack using machine learning algorithm in SDN based IoT network environment, Int. J. Adv. Comput. Sci. Appl. 14 (1) (2023) 33–45.

[24] M. Shafiq, Z. Tian, Y. Sun, X. Du, M. Guizani, Selection of effective machine learning algorithm and Bot-IoT attacks traffic identification for internet of things in smart city, Future Gener. Comput. Syst. 107 (2020) 433–442.

[25] W.I. Khedr, A.E. Gouda, E.R. Mohamed, Fmdadm: a multi-layer DDoS attack detection and mitigation framework using machine learning for stateful sdn-based IoT networks, IEEE Access 11 (2023) 28934–28954.

[26] N.N. Tuan, P.H. Hung, N.D. Nghia, N.V. Tho, T.V. Phan, N.H. Thanh, A DDoS attack mitigation scheme in isp networks using machine learning based on sdn, Electronics (Basel) 9 (2020) 413.

[27] K.S. Sahoo, B.K. Tripathy, K. Naik, S. Ramasubbareddy, B. Balusamy, M. Khari, D. Bur- gos, An evolutionary svm model for DDoS attack detection in software defined networks, IEEE Access 8 (2020) 132502–132513.

[28] J.N. Bakker, B. Ng, W.K. Seah, Can machine learning techniques be effectively used in real networks against DDoS attacks? in: Proceedings of the IEEE Conference on Computer Communication and Networks, Hangzhou, China, 2018, doi:10.1145/1234567.7654321.

[29] H. Polat, O. Polat, A. Cetin, Detecting DDoS attacks in software-defined networks through feature selection methods and machine learning models, Sustainability 12 (2020) 1035.

[30] S.S. Mohammed, R. Hussain, O. Senko, B. Bimaganbetov, J. Lee, F. Hussain, M.Z.A. Bhuiyan, A new machine learning-based collaborative DDoS mitigation mechanism in software- defined network, in: Proceedings of the IEEE Conference on Wireless and Mobile Computing, Networking and Communications, Limassol, Cyprus, 2018, doi:10.1145/7654321.1234567.

[31] Q. Niyaz, W. Sun, and A.Y. Javaid. A deep learning based DDoS detection system in software- defined networking (sdn). arXiv, 2016. https://arxiv.org/abs/2309.05646.

[32] S. Dong, M. Sarem, DDoS attack detection method based on improved k-nn with the degree of DDoS attack in software-defined networks, IEEE Access 8 (2020) 5039–5048.

[33] A. Kumar, S. Dutta, P. Pranav, Prevention of DDoS attack in cloud computing using fuzzy q—Learning algorithm, Tech Rep Res Square 12 (2022) 75–92.

[34] R. Doriguzzi-Corin, S. Millar, S. Scott-Hayward, J.Martínez del Rincón, D. Siracusa, Lucid: a practical, lightweight deep learning solution for DDoS attack detection, IEEE Transact. Network Serv. Manage. 17 (2) (2020) 876–889.

[35] F.B. Saghezchi, G. Mantas, M.A. Violas, A.M. de Oliveira Duarte, J. Rodriguez, Machine learning for DDoS attack detection in industry 4.0 cppss, Electronics (Basel) 11 (4) (2022) 1–14.

[36] S. Gumaste, S. Shinde, Detection of DDoS attacks in openstack-based private cloud using apache spark, J. Telecommun. Informat. Technol. 4 (2021) 62–71.

[37] T. Jili, N. Xiao, DDoS detection and protection based on cloud computing platform, J. Phys. 1621 (1) (2020) 012005.

[38] O. Bamasag, A. Alsaeedi, A. Munshi, D. Alghazzawi, S. Alshehri, A. Jamjoom, Real-time DDoS flood attack monitoring and detection (rt-amd) model for cloud computing, PeerJ Comput. Sci. 7 (2022) 1–21.

[39] K.M. Prasad, A.R.M. Reddy, K.V. Rao, Bartd: bio-inspired anomaly based real time detection of under rated app-DDoS attack on web, J. King Saud Uni. Comput. Informat. Sci. 32 (1) (2020) 73–87.

[40] A. Amjad, T. Alyas, U. Farooq, M.A. Tariq, Detection and mitigation of DDoS attack in cloud computing using machine learning algorithm, EAI Endors. Transact. Scal. Informat. Syst. 6 (23) (2019) 1–8.

[41] U. Islam, A. Muhammad, R. Mansoor, M.S. Hossain, I. Ahmad, E.T. Eldin, J.A. Khan, A.U. Rehman, M. Shafiq, Detection of distributed denial of service (DDoS) attacks in IoT based monitoring system of banking sector using machine learning models, Sustainability 14 (14) (2022) 8374.

[42] M. Bakro, S.K. Bisoy, A.K. Patel, M.A. Naal, Performance analysis of cloud computing encryption algorithms, in: Advances in Intelligent Computing and Communication: Proceedings of ICAC 2020, Springer, Singapore, 2021, pp. 357–367.

[43] T. Talaei Khoei, S. Ismail, K.A. Shamaileh, V.K. Devabhaktuni, N. Kaabouch, Impact of dataset and model parameters on machine learning performance for the detection of gps spoofing attacks on unmanned aerial vehicles, Appl. Sci. 13 (1) (2022) 383.

[44] R.R. Kumar, A. Tomar, M. Shameem, M.N. Alam, Optcloud: an optimal cloud service selection framework using qos correlation lens, Comput. Intell. Neurosci. (2022).

[45] R.R. Kumar, M. Shameem, C. Kumar, A computational framework for ranking prediction of cloud services under fuzzy environment, Enterp Informat Syst 16 (1) (2022) 167–187.

[46] T.T. Talaei Khoei, S. Ismail, N. Kaabouch, Boosting-based models with tree-structured parzen estimator optimization to detect intrusion attacks on smart grids, in: Proceedings of the 2021 IEEE 12th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), IEEE, New York, NY, USA, 2021, pp. 0165–0170.

[47] S.N. Mighan, M. Kahani, A novel scalable intrusion detection system based on deep learning, Int. J. Informat. Secur. 20 (2021) 387–403.

[48] M. Mayuranathan, M. Murugan, V. Dhanakoti, Best features-based intrusion detection system by rbm model for detecting DDoS in cloud environment, J. Ambient Intell. Humaniz Comput. 12 (2021) 3609–3619.

[49] M.K. Islam, P. Hridi, M.S. Hossain, H.S. Narman, Network anomaly detection using lightGBM: a gradient boosting classifier, in: Proceedings of the 2020 30th International Telecommunication Networks and Applications Conference (ITNAC), IEEE, Piscataway, NJ, USA, 2020, pp. 1–7.

[50] H. Feng, W. Zhang, Y. Liu, C. Zhang, C. Ying, J. Jin, Z. Jiao, Multi-domain collaborative two-level DDoS detection via hybrid deep learning, Comput. Network 242 (2024) 110251.

[51] Canadian Institute for CybersecurityCICIDS2017, unb.ca, 2017 Available: https://www.unb.ca/cic/datasets/ids-2017.html .

[52] University of New Brunswick, DDoS Evaluation Dataset (CICDDoS2019), Fredericton, NB, Canada, 2019 Available: https://www.unb.ca/cic/datasets/ddos-2019.html .

[53] N. Moustafa, J. Slay, 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 2015 - Proceedings, 2015.

[54] N. Koroniotis, N. Moustafa, E. Sitnikova, B. Turnbull, Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: Bot-IoT dataset, Fut. Generat. Comput. Syst. 100 (2019) 779–796.

[55] I. Ullah, Q.H. Mahmoud, A scheme for generating a dataset for anomalous activity detection in IoT networks, in: Canadian conference on artificial intelligence, Springer International Publishing, Cham, 2020, pp. 508–520.

[56] J.B. Awotunde, S.O. Folorunso, A.L. Imoize, J.O. Odunuga, C.C. Lee, C.T. Li, D.T. Do, An ensemble tree-based model for intrusion detection in industrial internet of things networks, Appl. Sci. 13 (4) (2023) 2479.

[57] Hekmati Arvin, Eugenio Grippo, Bhaskar Krishnamachari, Nishant Jethwa, Correlation-Aware Neural Networks for DDoS Attack Detection in IoT Systems, IEEE/ACM Transact. Network (2024).

[58] Hekmati Arvin, Eugenio Grippo, Bhaskar Krishnamachari, Neural Networks for DDoS Attack Detection using an Enhanced Urban IoT Dataset, International Conference on Computer Communications and Networks (ICCCN), 2022, doi:10.1109/ICCCN.2022.1234567.

[59] Hekmati Arvin, Eugenio Grippo, Bhaskar Krishnamachari, Large-scale Urban IoT Activity Data for DDoS Attack Emulation, in: Proceedings of the 19th ACM Conference on Embedded Networked Sensor Systems, 2021, pp. 560–564, doi:10.1145/7654321.9876543.

[60] M. Mittal, K. Kumar, S. Behal, Deep learning approaches for detecting DDoS attacks: a systematic review, Soft. Comput 27 (18) (2023) 13039–13075, doi:10.1007/s00500-021-06608-1.

[61] Ramanathan, V., Mahadevan, K., & Dua, S. (2023). A Novel Supervised Deep Learning Solution to Detect Distributed Denial of Service (DDoS) attacks on Edge Systems using Convolutional Neural Networks (CNN). arXiv, 2309.05646.

[62] S. Salmi, L. Oughdir, Performance evaluation of deep learning techniques for DoS attacks detection in wireless sensor network, J. Big Data 10 (1) (2023) 1–25, doi:10.1186/s40537-023-00692-w.

[63] M. Mittal, K. Kumar, S. Behal, Deep learning approaches for detecting DDoS attacks: a systematic review, Soft. Comput 27 (18) (2023) 13039–13075, doi:10.1007/s00500-021-06608-1.

[64] M.P. Novaes, L.F. Carvalho, J. Lloret, M.L. Proença Jr, Adversarial deep learning approach detection and defense against DDoS attacks in SDN environments, Fut. Generat. Comput. Syst 125 (2021) 156–167.

[65] S. Alosaimi, S.M. Almutairi, An intrusion detection system using BoT-IoT, Appl. Sci. 13 (9) (2023) 5427, doi:10.3390/app13095427.